UNIVERSITÉ DE GENÈVE

Archive ouverte UNIGE
https://archive-ouverte.unige.ch

Thèse 2013

Open Access

This version of the publication is provided by the author(s) and made available in accordance with the copyright holder(s).

Les sciences et les techniques comme moyens de preuve dans la procédure pénale : aspects techniques et juridiques de ces moyens de preuves

Friedrich, Cyrielle

How to cite

FRIEDRICH, Cyrielle. Les sciences et les techniques comme moyens de preuve dans la procédure pénale : aspects techniques et juridiques de ces moyens de preuves. Thèse, 2013. doi: 10.13097/archive-ouverte/unige:86032

This publication URL: https://archive-ouverte.unige.ch/unige:86032
Publication DOI: 10.13097/archive-ouverte/unige:86032

© This document is protected by copyright. Please refer to copyright holder(s) for terms of use.

LES SCIENCES ET LES TECHNIQUES COMME MOYENS DE PREUVE DANS LA PROCEDURE PENALE

ASPECTS TECHNIQUES ET JURIDIQUES DE CES MOYENS DE PREUVES

Par Cyrielle FRIEDRICH

Thèse de Doctorat

Sous la direction des Professeurs Alexandre FLÜCKIGER

et

Bernhard STRÄULI

(Références à jour au 8 mai 2016)

Faculté de droit de l'Université de Genève

Imprimatur No 914

TABLE DES MATIÈRES

REMERCIEMENTS 1
INTRODUCTION 3
PREMIERE PARTIE: LE CONTEXTE HISTORIQUE ET JURIDIQUE 5
CHAPITRE 1: LES DÉFINITIONS GÉNÉRALES ET L'ÉVOLUTION HISTORIQUE 5
I. Les définitions générales 5
A. La procédure pénale 5
B. La preuve 6
C. Les nouvelles technologies 7
II. L'évolution historique 7
A. Les procédures accusatoire, inquisitoire, mixte et l'administration de la preuve 8
1. Le système accusatoire 9
a. Les principes généraux 9
b. L'administration de la preuve en procédure accusatoire 9
2. Le système inquisitoire 11
a. Les principes généraux 11
b. L'administration de la preuve en procédure inquisitoire 12
3. Le système mixte 13
a. Les principes généraux 13
b. L'administration de la preuve en procédure mixte 15
B. Les nouvelles technologies 16
1. La dactyloscopie 16
a. La découverte des empreintes papillaires 16
b. La dactyloscopie comme moyen d'identification 16
c. Quelques chiffres démontrant l'importance des empreintes papillaires et du fichier AFIS en Suisse 18
2. L'acide désoxyribonucléique 19
a. La découverte de la molécule d'acide désoxyribonucléique 19
b. L'ADN comme moyen identificatoire 20
c. Le fichier CODIS et quelques chiffres sur l'empreinte génétique comme moyen identificatoire 21
3. Les moyens de télécommunication 23
a. La découverte de la téléphonie et son évolution 23
i. La découverte de la téléphonie fixe 23
ii. La téléphonie mobile 24
iii. La téléphonie IP 25
b. La téléphonie au service de la justice 26
4. La vidéosurveillance 26
a. De la photo à la vidéo 27
b. L'émergence de la vidéosurveillance 28
5. Le Global Positioning System 29
a. La naissance du GPS et son utilisation 29
b. L'utilisation du GPS comme moyen de surveillance 30
6. Les moyens informatiques 31
a. Le développement de l'ordinateur 31

b. La création d'Internet 33
c. L'Internet comme mode de communication 35
d. Les technologies de l'information au service de la police et de la justice 36
CHAPITRE 2: LE SIÈGE DE LA MATIÈRE 39
I. Le droit international *39*
A. Les instruments universels de protection des droits de l'homme *39*
1. La Déclaration universelle des droits de l'homme – DUDH 39
a. Sa place dans l'ordre juridique 39
b. Les droits devant idéalement être garantis 40
i. La DUDH et le droit de la preuve 40
ii. Quelques garanties essentielles en procédure pénale 41
c. Son champ d'application 42
2. Le Pacte international relatif aux droits civils et politiques – Pacte II 42
a. Sa place dans l'ordre juridique 42
b. Les droits garantis 43
i. Les similitudes entre le Pacte II et la DUDH 43
ii. Le Pacte II et les garanties procédurales 43
c. Son champ d'application 45
B. Les instruments régionaux de protection des droits de l'homme *46*
1. La Convention européenne des droits de l'homme – CEDH 46
a. Sa place dans l'ordre juridique 46
b. Les droits garantis 47
i. Les similitudes entre la CEDH, le Pacte II et la DUDH 47
ii. La possibilité de restreindre la garantie de la sphère privée 48
c. Le champ d'application 48
2. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – Convention STE n° 108 49
a. Sa portée juridique 49
b. Les droits garantis 50
c. Le champ d'application 51
II. Le droit interne *52*
A. Le droit fédéral *52*
1. La Constitution fédérale – Cst 52
a. Sa place dans l'ordre juridique 52
b. Les droits garantis 52
i. La Constitution et les droits fondamentaux en général 52
ii. La Constitution et les garanties procédurales 53
c. Le champ d'application 55
2. Les lois fédérales 56
a. Le Code de procédure pénale suisse – CPP 56
b. Les législations fédérales complémentaires 58
i. La loi sur la protection des données – LPD 58
ii. La loi sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues – Loi sur les profils d'ADN 59
iii. La loi sur la surveillance de la correspondance par poste et télécommunication – LSCPT 61
iv. La loi sur les systèmes d'information de police de la Confédération – LSIP 62
B. Le droit cantonal *63*

1. Les Constitutions cantonales....63
2. Les législations complémentaires....64
CHAPITRE 3: LA PREUVE – PRÉSENTATION GÉNÉRALE....67
I. L'objet de la preuve....67
II. La recherche de la vérité matérielle....68
III. La théorie générale de la preuve....69
A. La charge de la preuve et la présomption d'innocence....69
B. La liberté de la preuve et ses limites....71
1. Les principes....71
2. Les méthodes interdites de preuves....72
3. L'exploitation des moyens de preuves obtenus illégalement....73
a. Les preuves absolument inexploitables....74
b. Les preuves relativement inexploitables....74
c. La violation des règles d'ordre....75
d. L'effet en cascade de la règle d'exclusion....75
e. Le cas spécifique des preuves illégales recueillies par les particuliers....75
C. La libre appréciation, l'intime conviction et le doute....77
1. La libre appréciation des preuves....77
2. L'intime conviction et le doute....78
IV. Les différents moyens de preuves....79
A. Les constatations indirectes ou médiates....79
1. L'interrogatoire du prévenu....80
2. Le témoignage....81
3. Les personnes appelées à donner des renseignements....83
B. Les constatations directes ou immédiates....84
1. Les pièces à conviction....85
2. Les observations du lieu de l'infraction....86
C. Les constatations hybrides....87
1. L'expertise....87
2. Les procès-verbaux....89
DEUXIÈME PARTIE: LES NOUVELLES TECHNOLOGIES COMME MOYEN DE PREUVE....93
CHAPITRE 1: L'EXPERTISE....95
I. Les généralités....95
A. La définition et la notion....95
B. Le statut de l'expert....96
1. Le rôle de l'expert en procédure....96
a. L'expert et le témoin....96
b. L'expert et le juge....98
c. L'expertise et l'avis....98
d. L'expert comme auxiliaire de la justice....99
2. Le statut juridique de l'expert....100
a. Les relations entre l'expert et les parties....100
b. Les relations entre l'expert et la direction de la procédure....100
C. La portée de l'expertise....102
II. L'expertise en procédure pénale....104

A. La saisine de l'expert *104*
B. L'expertise judiciaire facultative *105*
1. Le choix de l'expert 105
a. Le droit de consultation des parties 105
b. Les conditions pour être expert 107
2. Le mandat d'expertise 109
a. La forme 109
b. Le contenu 110
3. La récusation et la révocation 111
a. Le principe 111
b. Les conséquences de la récusation et de la révocation 114
C. Le déroulement de l'expertise *115*
1. La communication de la mission et l'obligation d'accepter 115
2. L'exécution de l'expertise 116
3. La participation des parties à l'expertise 117
4. La rédaction et le dépôt du rapport d'expertise 118
III. L'appréciation et la valeur probante de l'expertise *120*
A. Le contrôle du juge et des parties *120*
B. L'appréciation du rapport d'expertise *122*
1. La direction de la procédure connaît le droit 122
2. L'évaluation des faits allégués 123
C. La valeur probante du rapport d'expertise *124*
1. La difficulté pour le juge de s'écarter du rapport d'expertise 124
2. L'évaluation de l'incertitude 127
CHAPITRE 2: LES PREUVES FONDÉES SUR LES SCIENCES 129
I. La dactyloscopie *130*
A. L'introduction *130*
1. Définition de l'empreinte papillaire 130
a. L'immuabilité 131
b. L'inaltérabilité 132
c. L'individualité 133
2. Le prélèvement et l'analyse des empreintes papillaires 134
a. La recherche et la révélation des empreintes 134
b. L'analyse 136
c. Le processus identificatoire de la comparaison à l'achèvement 137
i. L'assistance des outils automatisés 137
ii. La comparaison manuelle 139
iii. Le résultat identificatoire 140
B. Les notions juridiques *142*
1. Le cadre légal 142
a. L'atteinte aux droits fondamentaux du prélèvement et de l'analyse des données signalétiques 142
b. Les dispositions suisses sur les données signalétiques 143
i. La saisie des empreintes papillaires 144
a) Le champ d'application matériel et personnel 144
b) La compétence pour ordonner la saisie 145
c) Le refus et les voies de recours 146

ii. L'enregistrement dans AFIS 147
a) Le traitement des empreintes digitales et palmaires 147
b) L'utilisation des données enregistrées dans AFIS 148
iii. La conservation et la destruction d'une fiche signalétique dans AFIS 149
a) La conservation des données signalétiques au sens de l'art. 261 CPP 149
b) La conservation des données selon l'Ordonnance réglementant l'AFIS 150
c) La destruction des données signalétiques 152
2. L'identification judiciaire et la preuve dactyloscopique 152
a. La nature déterministe de l'identification 153
i. L'absence de consensus international et les résolutions de l'association professionnelle internationale pour l'identification (IAI) 153
ii. L'identification dactyloscopique en Suisse 154
b. La valeur probatoire 156
i. La valeur probatoire scientifique reconnue 156
ii. La preuve dactyloscopique et le faisceau d'indices 158
C. La discussion sur la preuve dactyloscopique 159
1. L'évaluation de la preuve dactyloscopique dans l'ordre judiciaire suisse 159
a. Le potentiel de la preuve dactyloscopique 159
i. Une preuve hybride 159
ii. La reconnaissance scientifique 160
iii. Les facultés probatoires à charge ou à décharge 162
iv. L'univocité de l'univers déterministe 162
b. Les problématiques liées à l'exploitation et à l'administration de la preuve dactyloscopique 163
i. L'absence de standard minimum 163
ii. L'expérience comme condition requise à l'évaluation des traces papillaires 166
iii. Les risques d'erreur 168
iv. Le manque de formation scientifique des juristes 171
v. Les limites de l'approche déterministe 173
2. Une nouvelle perspective: la nature probabiliste de l'identification 174
a. La démonstration relative de la réalité par l'approche déterministe 174
b. La théorie de la nature probabiliste 175
c. L'avantage des probabilités 176
3. L'utilisation du système AFIS et ses limites 177
a. Un outil efficace et précieux pour les dactyloscopes et la justice 177
b. Le traitement informatisé des empreintes papillaires à la lumière de la liberté personnelle et de la sphère privée 179
c. L'exception de l'art. 261 al. 2 CPP 181
i. Le passé, le présent et le futur possible du champ d'application personnel 181
ii. La légalité de l'exception de l'art. 261 al. 2 CPP 184
d. La durée de conservation 187
D. La synthèse des débats et conclusion 188
II. L'acide désoxyribonucléique 190
A. L'introduction 190
1. Définition de l'ADN 191
2. Où trouve-t-on de l'ADN? 193
3. Les trois qualités fondamentales des traces ADN et du profil génétique 194
a. La pérennité 194

b. L'inaltérabilité 195
c. L'individualité 195
4. Le prélèvement du matériel biologique 196
a. La recherche et le prélèvement du matériel génétique 197
i. Les traces indiciaires ou le prélèvement sur la scène de crime 197
ii. Le prélèvement sur l'individu ou de type corporel 198
b. L'analyse, la comparaison et l'identification des profils génétiques 198
c. Le processus identificatoire et l'assistance de la base de données CODIS 200
B. Les notions juridiques 201
1. Le cadre juridique 201
a. Les droits fondamentaux 202
i. L'atteinte à l'intégrité corporelle et à la liberté personnelle causée par le prélèvement 202
ii. L'atteinte à la liberté personnelle, particulièrement à l'autodétermination informationnelle, causée par l'établissement du profil d'ADN et de son intégration dans CODIS 203
iii. L'admissibilité de la restriction aux droits fondamentaux touchés par le prélèvement et l'analyse ADN 203
b. La réglementation nationale applicable à l'identification par l'ADN 205
i. Le prélèvement d'ADN 205
a) Le champ d'application matériel 205
b) Le champ d'application personnel 207
c) La compétence 210
d) L'exécution de la mesure 212
ii. L'établissement d'un profil d'ADN et son intégration dans CODIS 212
iii. La conservation des données génétiques 214
a) La destruction des échantillons 214
b) L'effacement des profils d'ADN 215
2. L'identification judiciaire 217
a. La nature scientifique et identificatrice de l'ADN 217
b. La nature probabiliste de la preuve 218
i. La théorie de la coïncidence fortuite et la population de référence 218
ii. Le rapport de vraisemblance et le modèle bayésien 220
c. La valeur probatoire 221
C. La discussion sur la preuve génétique 223
1. L'évaluation de la preuve génétique dans l'ordre juridique suisse 224
a. Le potentiel de la preuve génétique 224
i. Les qualités scientifiques de la preuve par l'ADN 224
ii. Les atouts du matériel génétique analysable 225
iii. L'assurance de qualité de l'expertise 227
iv. La nature probabiliste des résultats d'expertise 227
b. Les problématiques liées à l'exploitation et à l'administration de la preuve génétique 228
i. L'unicité relative du profil génétique 228
a) Le cas des vrais jumeaux 228
b) Le cas des coïncidences fortuites 229
c) Le cas des proches parents 230
ii. Les risques d'erreurs liés à l'échantillon 231
a) Le transfert d'ADN 231
b) Le mélange et la dégradation 234

c) La contamination 235
d) Les autres facteurs 237
iii. Les limites des probabilités et le manque de formation des juristes 238
a) Les limites des probabilités 239
b) Le manque de formation des juristes 240
iv. Le renversement du fardeau de la preuve 241
2. L'utilisation du système CODIS et ses limites 242
a. L'efficacité et les avantages du système automatisé CODIS 243
i. Un outil d'enquête et d'entraide à la poursuite pénale 243
ii. L'atteinte aux libertés fondamentales partiellement amoindrie 244
a) La limitation possible des enquêtes de grandes envergures 244
b) Les avantages de l'anonymisation 245
c) La limitation des ingérences à la sphère privée des individus innocents 245
b. Les risques liés à l'utilisation et à la croissance de CODIS 246
i. La négligence des autres éléments de l'enquête 246
ii. La sécurité du fichier informatisé 247
c. Le profilage ADN automatisé à la lumière de la liberté personnelle et de la sphère privée 248
i. La présomption d'innocence 248
ii. Le droit à l'autodétermination informationnelle et la sphère privée 249
iii. La proportionnalité des atteintes aux droits fondamentaux liées à l'utilisation de CODIS 250
d. Les recommandations pour l'avenir 252
i. Le décryptage de la partie codante de l'ADN 252
ii. L'intégration de profils d'ADN d'auteurs de contraventions 253
D. La synthèse des débats et conclusion 254
CHAPITRE 3: LES PREUVES FONDÉES SUR LES TECHNIQUES 257
I. Les techniques de la surveillance 258
A. La surveillance des télécommunications 258
1. L'introduction 259
a. Définition de la surveillance de la correspondance par télécommunication 259
b. Les deux types de surveillance des télécommunications 259
c. Le contexte technique de la surveillance des télécommunications 261
2. Le cadre légal 262
a. Les droits fondamentaux, les libertés et leur protection 262
i. La protection des communications et l'atteinte aux droits fondamentaux issus de la surveillance des télécommunications 262
ii. La restriction admissible des droits fondamentaux touchés par la surveillance secrète des télécommunications 263
b. La protection du Code pénal 266
i. Les infractions du Code pénal 266
ii. L'exclusion de l'application des art. 179bis et ter CP 267
c. Les normes fédérales élémentaires à la surveillance répressive des télécommunications 268
i. Le champ d'application 268
ii. Les conditions d'application 269
a) Pour la surveillance des communications 269
1. L'existence de graves soupçons 269
2. La justification au regard de la gravité de l'infraction 270
3. La subsidiarité de la mesure 271

4. Le catalogue limitatif des infractions susceptibles de justifier une surveillance 271
b) Pour l'obtention des données relatives au trafic et à la facturation et identification des usagers..272
iii. Les objets de la surveillance de la correspondance par télécommunication 272
iv. La procédure de mise sous surveillance des télécommunications 274
a) Les compétences pour ordonner et autoriser la mesure de surveillance.....274
b) La procédure d'autorisation et autorisation-cadre 274
c) L'exécution de la mesure.....276
1. Le Service de surveillance de la correspondance par poste et télécommunication (SCPT).....276
2. Les fournisseurs de services de télécommunication et d'accès internet.....277
d) La levée de la surveillance 278
e) La communication au prévenu et aux tiers sujets de la surveillance.....279
v. L'exploitation des données recueillies 280
a) La protection du secret professionnel 280
b) Les informations non-nécessaires à la procédure pénale 282
c) Les informations recueillies lors d'une surveillance non-autorisée 283
d) Les découvertes fortuites 283
e) Les données exploitables.....285
d. Les normes élémentaires à la surveillance privée des télécommunications 285
3. L'usage et le moyen probatoire 287
a. L'utilisation des informations recueillies.....287
i. En cas de surveillance répressive ou mixte.....287
ii. En cas de surveillance préventive 289
iii. En cas d'écoute ou d'enregistrement effectué par des particuliers 289
b. Les données issues de la surveillance des télécommunications comme moyen de preuve.....290
4. La discussion sur la preuve obtenue à l'aide de la surveillance des télécommunications.....291
a. Le potentiel de la surveillance des télécommunications 291
i. La technicité de la preuve obtenue par le biais de la surveillance 291
ii. La difficulté de nier l'évidence d'une information issue de la surveillance 292
iii. L'efficacité des moyens de surveillance 293
b. Les problématiques liées à l'exploitation et à l'administration des informations issues de la surveillance des télécommunications 294
i. La surveillance incomplète 294
ii. La séparation des données utiles et inutiles à la procédure pénale en cours 296
a) Le problème du dossier fantôme contenant les données issues de la surveillance et écartées du dossier de procédure 296
b) La modification possible des données recueillies 297
iii. La traduction et l'interprétation des communications échangées.....298
a) La traduction des communications.....298
b) L'emploi de langage codé par les personnes surveillées.....299
c. Quelques pistes de réflexion 300
i. La surveillance des communications VoIP 300
a) La technologie VoIP et les chevaux de Troie 300
b) Les normes actuelles sont-elles suffisantes pour autoriser l'utilisation des logiciels espions?.....301
c) La révision de la LSCPT et l'introduction de l'art. 269ter CPP 304
1. Le projet de modification de la LSCPT en quelques mots 304
2. La création de l'art. 269*ter* CPP 305

d) Les risques de l'utilisation des chevaux de Troie pour la valeur probante des données recueillies 309
ii. La surveillance préventive 311
a) La réglementation prévue par le CPP 311
b) La réglementation prévue dans la LMSI 311
c) Les réglementations cantonales sur la police 312
d) La loi sur le renseignement (LRens), non-entrée en vigueur 315
iii. L'IMSI- Catcher 317
a) La technique de l'IMSI-Catcher en quelques mots 317
1. La description de l'IMSI-Catcher 317
2. Les limites techniques 317
b) L'utilisation de l'IMSI-Catcher au regard du droit suisse 318
B. La vidéosurveillance 322
1. L'introduction 322
a. La définition de la vidéosurveillance 322
b. Les divers types de vidéosurveillance 323
i. La vidéosurveillance exercée par les personnes privées et par les autorités publiques 323
ii. La finalité de la vidéosurveillance 324
iii. L'agencement du système de vidéosurveillance 325
iv. Excursus: l'enregistrement audiovisuel 327
c. Le contexte technique de la vidéosurveillance 328
2. Le cadre légal 329
a. Les droits fondamentaux, les libertés et leur protection 330
i. La protection des droits fondamentaux et l'atteinte aux libertés causée par la vidéosurveillance 330
a) La liberté personnelle 331
b) Le droit au respect de la sphère privée 332
c) Le droit d'être protégé contre l'emploi abusif de ses données personnelles 333
d) La liberté de réunion 333
e) La dignité humaine 334
ii. La restriction admissible des droits fondamentaux touchés par la vidéosurveillance 334
b. La protection du Code pénal 338
c. Les normes fédérales et cantonales élémentaires à la vidéosurveillance 339
i. La vidéosurveillance effectuée par les particuliers 340
a) L'art. 28 CC 340
b) L'art. 179quater CP 341
c) Les principes généraux de la LPD et l'applicabilité des art. 12 ss LPD 341
1. Le principe de licéité (art. 4 al. 1 LPD) 342
2. Le principe de proportionnalité (art. 4 al. 2 LPD) 343
3. Le principe de bonne foi (art. 4 al. 2 LPD) 345
4. Le principe de finalité (art. 4 al. 3 LPD) 345
5. Le principe de sécurité des données 346
ii. La vidéosurveillance effectuée par les autorités 346
a) La vidéosurveillance dissuasive du domaine privé ou secret 346
b) La vidéosurveillance dissuasive des espaces publics 347
1. L'exercice de la vidéosurveillance dissuasive par les organes fédéraux 347
2. L'exercice de la vidéosurveillance dissuasive par les autorités cantonales 349
c) La vidéosurveillance invasive du domaine privé ou secret 350

d) La vidéosurveillance invasive des espaces publics 352
1. Les conditions d'application....352
2. La communication à la personne observée 353
3. L'exploitation des informations obtenues, des découvertes fortuites et des preuves obtenues illégalement 354
4. La fin de l'observation....355
3. L'usage et le moyen probatoire 355
a. L'efficacité de la vidéosurveillance dissuasive 356
b. Les informations recueillies par vidéosurveillance et leur valeur probatoire....357
4. La discussion sur la preuve obtenue par vidéosurveillance 358
a. Le potentiel de la vidéosurveillance....358
i. La nature de la preuve obtenue par vidéosurveillance ou technique audio-visuelle 358
ii. La vidéosurveillance comme un moyen de preuve à charge ou à décharge....359
iii. Les procédés techniques limitant la portée et la capture réalisées par les caméras....361
a) La détection de mouvements....361
b) La vidéosurveillance intelligente 362
c) La réduction du champ de vision 362
d) La destruction automatique des informations captées et enregistrées 363
b. Les problématiques liées à la preuve issue de la vidéosurveillance 363
i. La qualité des images et leur modélisation bidimensionnelle....363
a) La manipulation des images 363
b) Le traitement des images....364
c) La visualisation en deux dimensions d'une réalité en trois dimensions....365
1. La problématique de la vision en deux dimensions....365
2. La modélisation tridimensionnelle 366
ii. Les pertes d'informations liée à une surveillance incomplète ou aux données retirées....366
a) La problématique des angles morts....367
b) L'étendue du champ de vision dépendamment de l'utilisation d'une caméra fixe ou mobile....367
c) Les erreurs d'interprétation des images 368
iii. Une valeur ajoutée, mais non pas un moyen d'investigation unique....369
c. Quelques pistes de réflexion 371
i. Quelques moyens de précautions à mettre en œuvre....371
a) Les méthodes techniques....371
b) Les conditions de mise en œuvre ou organisationnelles....372
ii. L'adoption ou la modification des bases légales en matière de vidéosurveillance dissuasive exercée par les autorités ou les particuliers et de la surveillance répressive opérée par les personnes privées 373
II. Les techniques de localisation 374
A. Les principes généraux....374
1. La définition de la géolocalisation....374
2. Le champ d'étude 375
a. Les services basés sur la localisation géographique 375
b. La géolocalisation en Suisse via la téléphonie mobile et les installations GPS....376
c. La localisation ou le suivi spatio-temporel 376
B. Le contexte technique....377
1. La localisation à l'aide de la technologie GPS....377
a. Le système de navigation par satellite et les données fournies....377
b. Le cas particulier des boîtes noires et du système ISA....378

i. Intelligent Speed Assistance 378
ii. Le programme Via sicura 379
2. La localisation lors d'une surveillance de la télécommunication mobile 380
a. La localisation à l'aide du réseau de téléphonie mobile 381
i. Les systèmes de téléphonie 381
ii. La localisation des téléphones portables à l'aide des antennes relais 382
b. Le cas particulier de la recherche par champ d'antennes ou balayage d'antennes 384
C. Le cadre légal 384
1. Les droits fondamentaux, les libertés et leur protection 384
a. Les principes pertinents 385
b. Le respect de la vie privée en cas de localisation GPS 386
c. La nature de l'atteinte à la vie privée 387
2. La justification de l'ingérence 388
a. L'existence d'une loi et la prévisibilité de la norme 388
i. La procédure de mise sous surveillance au moyen des systèmes de navigation par satellite 389
a) La prévisibilité de la loi 389
b) La procédure et les garanties contre les abus 389
c) La surveillance par GPS à but préventif et la surveillance rétroactive 391
d) Les divergences entre la surveillance par GPS et l'observation 391
ii. La procédure de mise sous surveillance au moyen des systèmes d'antennes relais 392
a) La différence entre les dispositifs employant les systèmes mondiaux de navigation par satellite et le système de téléphonie 392
b) Le dispositif légal pour la localisation à l'aide d'appareils de téléphonie mobile 393
1. Le positionnement d'un téléphone mobile déterminé 393
2. La recherche par champ d'antennes 394
iii. La mise sous surveillance au moyen des systèmes de navigation par satellite ou d'antennes relais par les particuliers 396
b. Le but et la nécessité de l'ingérence 396
D. Les données de localisation comme moyen de preuve 397
E. La discussion sur la preuve liée aux moyens de localisation 398
1. Le potentiel des preuves issues des systèmes de localisation 398
a. La nature technique de la preuve et son administration à charge ou à décharge 398
i. Les données mathématiques 399
ii. Une preuve à charge ou à décharge 399
b. La connaissance des données de positionnement 399
c. Les autres possibilités offertes à l'aide des données de positionnement 401
i. L'utilité du géopositionnement pour l'exécution des peines 401
ii. Une aide à l'enquête 402
iii. Le système des boîtes noires ou ISA et le projet Via sicura 402
iv. La recherche par champ d'antennes 403
2. Les faiblesses et problématiques des preuves issues des systèmes GPS et GSM 404
a. L'interprétation nécessaire des résultats de positionnement 404
i. En cas de correspondance positive 405
ii. En cas de correspondance négative 405
iii. Le travail d'enquête 406
b. L'approximation de la localisation 407
i. Les données issues des systèmes de navigation par satellite 407

ii. Les données issues des systèmes de télécommunication mobile 409
c. Les dangers potentiels et les techniques de sécurité 410
i. Les problèmes techniques fréquents et leurs conséquences 410
ii. Les pannes survenant sur les systèmes GPS ou de téléphonie mobile 410
iii. Le piratage des données GPS et/ou GSM 411
3. L'émergence des puces RFID 412
a. Le système d'identification par radiofréquence (RFID) 412
i. La technologie RFID 412
ii. Le fonctionnement de la technologie RFID 413
iii. Les évolutions et applications récentes de la RFID 414
b. L'exploitation des puces RFID par l'autorité pénale et sa légalité 415
i. Les types de localisation grâce à la technologie RFID 415
a) La localisation passive 415
b) La localisation active 416
ii. La légalité en droit suisse de la géolocalisation à l'aide de la RFID 416
c. Les difficultés ou obstacles liés à l'utilisation de la RFID comme moyen de localisation et moyen de preuve 417
i. La sécurité du système de fonctionnement RFID 417
ii. Les obstacles au succès de la RFID 418
iii. L'emploi comme moyen probatoire des données issues de la technologie RFID 419
III. Les techniques informatiques et les systèmes de gestion de base de données 419
A. Les moyens informatiques 420
1. L'introduction 420
2. Quelques notions techniques et définitions 421
a. Le réseau internet et les groupes de discussion 421
b. L'identification des appareils électroniques sur le réseau 422
i. Le protocole TCP/IP et l'adresse IP 422
a) Les notions techniques 422
b) L'adresse IP est-elle une donnée personnelle? 423
ii. L'adresse MAC 423
c. Les supports informatiques 424
3. Le cadre juridique 424
a. Les droits fondamentaux, les libertés et leur protection 424
i. La surveillance sur Internet et l'atteinte aux libertés personnelles 425
a) En cas d'observation 425
b) En cas d'investigation secrète et de recherches secrètes 426
ii. La perquisition des documents, l'atteinte à la vie privée et au droit au respect du domicile 427
b. La protection du Code pénal 428
i. La soustraction de données (art. 143 CP) 428
ii. L'accès indu à un système informatique (art. 143bis CP) 429
iii. La violation des art. 179 à 179quater et 179novies CP en cas de surveillance par l'autorité 430
c. Les normes justifiant l'atteinte aux droits fondamentaux 432
i. En cas de surveillance sur Internet 433
a) L'observation 434
b) L'investigation secrète 435
1. L'investigation secrète 435
2. La notion d'agent infiltré et délimitation 437

3. Les conditions matérielles....438
a) L'existence de soupçon de la commission d'une infraction énumérée à l'alinéa 2....438
b) La justification de la mesure au regard de la gravité de l'infraction....439
c) La subsidiarité de la mesure....440
4. Les conditions formelles....440
a) La procédure d'autorisation....440
b) Les constatations fortuites....441
5. Les limites....441
a) De la mission....441
b) Le sort des preuves....442
6. La fin de l'investigation secrète....443
c) Les recherches secrètes....443
1. La modification du Code de procédure pénale suisse entrée en vigueur le 1er mai 2013....443
2. Les recherches secrètes....445
a) Le champ d'application....445
b) Les conditions matérielles et formelles....445
c) Les limites des nouvelles dispositions légales sur les recherches secrètes et l'investigation secrète....447
ii. En cas de surveillance de l'accès Internet....448
iii. La perquisition des documents électroniques....449
a) Le champ d'application....450
b) L'ordre de perquisition....450
1. Compétence, forme et contenu de l'ordre de perquisition....450
2. Les conditions à respecter pour la perquisition des documents et enregistrements....451
c) L'exécution de la perquisition....452
1. Les dispositions générales....452
2. Les dispositions spéciales....453
d) Les données recueillies....454
1. Les données informatiques utiles....454
2. La mise sous scellé....455
3. Les découvertes fortuites....456
4. L'efficacité et l'utilisation comme preuve des données informatiques....457
a. L'utilité de la surveillance sur Internet et les moyens de preuves issus de cette surveillance....457
b. L'utilité de la surveillance de l'accès Internet avec l'obtention des informations concernant l'adresse IP ou l'adresse MAC....459
c. L'utilité de la perquisition des documents électroniques et leur exploitation comme moyen de preuve.460
d. La conclusion sur l'efficacité et l'utilisation comme preuve des moyens informatiques....461
5. La discussion sur la preuve informatique....461
a. Les problématiques liées à la surveillance sur Internet....462
i. L'incapacité de surveiller Internet de manière préventive....462
a) Les changements depuis l'entrée en vigueur du CPP....462
b) La conséquence de la nouvelle réglementation sur les enquêtes réalisées sur un chatroom ou un forum de discussion....463
ii. Les données interceptées par un Cheval de Troie introduit par l'autorité pénale....464
iii. Le vol d'identité et des accès....464
b. Les problématiques liées à la surveillance de l'accès Internet....466

i. L'accès Internet depuis un réseau public, depuis un cybercafé, depuis le domicile d'un tiers ou par l'intermédiaire d'un routeur....466
a) L'accès depuis un réseau public, un cybercafé ou le réseau d'une entreprise....466
b) En cas d'utilisation d'un accès Internet familial ou d'un tiers....467
ii. L'accès Internet non sécurisé....468
iii. La duplication des adresses IP et/ou de l'adresse MAC....469
c. Les données issues de la perquisition sur un support informatique....470
i. La vulnérabilité des systèmes d'exploitation....470
ii. L'incapacité générale d'authentifier les données informatiques....471
6. Une perspective d'avenir – L'espion clavier....472
a. Qu'est-ce que l'espion clavier?....473
b. L'utilité de l'espion clavier en procédure pénale....473
c. L'évolution du espion clavier avec l'espionnage à distance à l'aide des ondes électromagnétiques....474
B. Les bases de données....475
1. L'avènement des systèmes d'information....475
a. Les remarques générales....475
i. Quelques notions techniques....476
ii. La transmission des informations à distance....476
iii. Les généralités sur les données enregistrées, traitées et analysées....477
b. L'introduction des bases de données dans l'administration et dans le cadre des tâches des autorités en procédure pénale....478
2. Quelques bases de données fédérales....479
a. Le système informatisé de la Police judiciaire fédérale – JANUS....479
b. Le système de recherches informatisées de police – RIPOL....481
c. Le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police – IPAS....482
d. Le système automatisé d'identification des empreintes digitales – AFIS....482
e. La banque de données nationale sur les profils d'ADN – CODIS....483
f. Quelques autres bases de données....483
3. L'utilisation des bases de données et la protection des données personnelles....484
a. Les atteintes à la sphère privée et à l'autodétermination informationnelle....484
i. Quelles menaces pour la vie privée et les libertés fondamentales?....484
ii. Comment limiter des ingérences inacceptables et les craintes suscitées par l'exploitation des bases de données?....486
a) Les principes généraux....486
b) La surveillance, la transparence et l'harmonisation des procédures....486
1. La surveillance de la gestion des bases de données....487
2. Le devoir d'informer....487
3. Le droit d'accès....487
a. Le droit d'accès en dehors d'une procédure pénale....488
b. Le droit d'accès dans le cadre d'une procédure pénale pendante....488
4. L'harmonisation des procédures....489
b. L'utilité des bases de données....490
4. La fiabilité des bases de données dans la recherche criminelle....491
a. Les risques humains....491
i. L'adéquation et la qualité des données....491

ii. Le vol, la perte de maîtrise des informations de connexion et la malveillance des utilisateurs des bases de données 492
b. Les risques techniques 493
5. Des perspectives d'avenir – Quelques orientations possibles de l'exploitation des bases de données par les autorités pénales 494
a. Les données biométriques comme aide à l'investigation criminelle 494
i. La reconnaissance faciale des images de vidéosurveillance 494
ii. La reconnaissance vocale des enregistrements issus de la surveillance des télécommunications 495
b. Le potentiel inexploité du mode Light out par le système automatique d'identification des empreintes digitales 496
IV. La synthèse des débats et conclusion 497
A. Les constatations générales 497
B. Les lacunes législatives depuis l'entrée en vigueur du Code de procédure pénale 498
C. La procédure différenciée pour ordonner une mesure de surveillance, l'utilisation d'un autre dispositif technique, l'observation, l'investigation secrète et les recherches secrètes 499
TROISIEME PARTIE: LA CONCLUSION ET LES PROPOSITIONS 501
CHAPITRE 1: SOMMES-NOUS FACE A UNE NOUVELLE CONCEPTION DU SYSTEME PROBATOIRE? 503
I. L'importance des preuves scientifiques ou techniques 503
A. La reconnaissance des nouvelles technologies comme preuve de la vérité 504
B. L'administration des nouvelles technologies et l'appréciation de la preuve 504
II. La stratégie du doute ou la décrédibilisation des preuves scientifiques ou techniques 505
III. L'impact des preuves issues des nouvelles technologies et de la stratégie du doute sur la décision du juge 506
CHAPITRE 2: LA COLLABORATION ENTRE LES AUTORITES PENALES ET LES EXPERTS EST-ELLE ADEQUATE? 509
I. La confiance des juristes portée aux experts 509
A. Le principe de confiance 509
B. Les bases de la confiance 509
1. L'impartialité et l'indépendance des experts 509
2. L'accréditation des laboratoires et l'expérience des experts 510
3. La reconnaissance technique et scientifique 510
C. Le manque de connaissances scientifiques ou techniques des magistrats 510
II. Le manque d'interprétation renforçant le rôle de l'expert 511
III. Les propositions 512
A. La formation des juristes 512
B. La formation des experts au monde judiciaire et au vocabulaire des juristes 513
C. L'amélioration de la communication entre les autorités pénales et les experts 513
LA CONCLUSION FINALE 515
GLOSSAIRES I
BIBLIOGRAPHIE VII
ABREVIATIONS LIII

REMERCIEMENTS

Lorsque nous nous lançons dans un travail de doctorat, nous pensons qu'il s'agit d'un travail solitaire. Je suis aujourd'hui convaincue du contraire. Un grand nombre de personnes m'ont permis d'arriver au bout de cette thèse. Merci à tous et plus spécialement…

Je souhaite exprimer ma gratitude à mes directeurs de thèse, Messieurs les Professeurs Bernhard Sträuli et Alexandre Flückiger, pour leur aide et leur soutien apporté durant ces années de doctorat. Je remercie également Messieurs les Professeurs Christophe Champod et Christian Bovet pour l'honneur qu'ils m'ont fait en acceptant de participer à mon jury de thèse ainsi que pour leurs précieux conseils.

Je sais infiniment gré à Messieurs Jean-Pascal Chavanne, Provider Management au Centre de services informatiques du Département fédéral de justice et police, Christian Gehrig, Responsable opérationnel à l'unité de génétique forensique du Centre universitaire romande de médecine légale de Genève, et Axel Glaeser, Chef de division du service AFIS ADN, de m'avoir reçu au sein de leur Service et/ou Département ainsi que de s'être rendus disponibles pour me fournir toutes les clés techniques et scientifiques utiles à ma recherche.

Ces remerciements seraient incomplets si je ne m'adressais pas à mes proches, amis et famille, dont le soutien affectif m'a permis de gravir toutes ces étapes, leur présence durant ces années de doctorat et à ma soutenance m'a touchée. Je remercie plus particulièrement Maria, pour sa gentillesse, sa force et sa disponibilité pour la relecture, Adrian, pour les encouragements ainsi que pour les moments de pauses à se changer les idées , et ma sœur, Lauriane, pour l'apport de ses connaissances médicales et son soutien moral, je sais qu'il n'a pas toujours été simple de me supporter dans tout ce que j'ai entrepris, mais tu as été là. Ma reconnaissance est grande.

Enfin, je tiens particulièrement à remercier mes parents qui n'ont jamais douté de moi, qui sont restés présents à chaque étape, qui m'ont soutenue à bout de bras durant les moments d'incertitudes, de découragement ou de consternation de voir le temps qui file, mais aussi de joie où l'on partageait les sourires d'une étape franchie, et dont les encouragements ont été indéfectibles du premier mot de mon écrit au point final, à ma soutenance de thèse jusqu'aux corrections. Chaque mot est trop faible pour exprimer ma gratitude et mon affection, vous êtes mon plus grand soutien. Maman, Papa, vous êtes les piliers fondateurs de ce que je suis et de mes réussites. Un énorme merci pour tout, ce travail est aussi le vôtre.

INTRODUCTION

1 La présomption d'innocence avec son corollaire – l'administration des preuves – est au cœur du procès pénal en Suisse. Afin de rechercher la vérité matérielle, le juge a le pouvoir de librement apprécier les preuves qui lui sont soumises sans être limité par un *numerus clausus* des moyens probatoires.

2 Depuis quelques années, les nouveautés scientifiques et technologiques passionnent le grand public et les autorités pénales. Accompagnant cette évolution, l'exploitation des sciences et des techniques comme mode probatoire s'est démocratisée, mais non sans difficulté.

3 La complexité des nouvelles technologies requiert des connaissances particulières pour traiter, analyser et interpréter les indices. Face à ces preuves, le juge recourt fréquemment aux experts – criminologues, police scientifique et police technique – pour l'aider dans l'interprétation et la compréhension des indices. Ainsi, les nouvelles technologies sont des moyens de preuves modernes et l'expertise est leur mode d'interprétation.

4 L'explosion des preuves relevant des nouvelles technologies s'est accompagnée également d'un mouvement populaire soutenant la crédibilité des sciences et des techniques. Faussé par des séries comme les "Experts", le *quidam* pense que l'ADN ou les empreintes digitales fournissent facilement et rapidement un résultat identificatoire avec une force probante extrême au point de, généralement, pousser l'auteur à faire des aveux.

5 En outre, beaucoup d'individus estiment que les sciences et les techniques par leur matérialisation et leur logique protègent la preuve pénale contre l'erreur, contre une éventuelle pression des enquêteurs et contre la subjectivité.

6 La présentation romancée des nouvelles technologiques, notamment, par des séries à succès, et l'objectivité des sciences et des techniques ont poussé certaines personnes à estimer que la preuve issue des nouvelles technologies a une valeur probante sans égale qui contribue incontestablement et avec fiabilité à la recherche de la vérité matérielle.

7 Ces constats et l'importance de la preuve au cœur du procès pénal nous ont amené à nous interroger sur l'intégration des nouvelles technologies.

8 Quelles sont les nouvelles technologies qui intéressent la procédure pénale? Comment sont-elles réglementées au sein du Code de procédure pénale? Cette réglementation est-elle exhaustive, adéquate et/ou suffisante? Quels sont les avantages et les risques de leur

utilisation comme preuve? Enfin, le juge peut-il appréhender facilement les subtilités techniques des diverses méthodes probatoires issues des nouvelles technologies?

9 Après avoir éclairé ces quelques points, deux ultimes questions se poseront: sommes-nous face à une nouvelle conception du système probatoire qui consacrerait la preuve scientifique ou technique comme une nouvelle *probatio probatissima*? La collaboration entre l'autorité policière, les magistrats et les experts est-elle adéquate ou la décision du juge est-elle dictée par le rapport d'expertise et l'avis du spécialiste?

10 Pour pouvoir nous positionner, nous devons au préalable examiner les procédés scientifiques ou techniques et leur perception par le monde judiciaire. Dans cet objectif, notre étude est divisée en trois parties: le contexte historique et juridique de la preuve pénale (Partie I), les nouvelles technologies et la procédure pénale (Partie II), les conclusions et propositions (Partie III).

11 Dans la première partie, après avoir défini les trois sujets au cœur de notre étude – la preuve, la procédure pénale et les nouvelles technologies – nous exposerons le cadre historique, le siège de la matière et les principes généraux régissant la preuve pénale.

12 Dans la seconde partie, nous analyserons diverses technologies sous l'angle scientifique ou technique et sous l'angle juridique. L'aspect technico-scientifique tente de fournir les éléments essentiels techniques pour permettre aux professionnels du droit d'appréhender le fonctionnement des nouvelles technologies. Ces éléments sont purement théoriques assortissant parfois une perfection à la science ou la technique considérée qui n'est pas absolue en pratique, comme nous le verrons au moment des discussions sur les qualités et défauts de ces modes de preuve. L'aspect juridique cible l'exploitation de ces moyens probatoires en procédure pénale. Ces analyses doivent permettre de dégager les points positifs et négatifs des moyens de preuves. A noter que le nombre de sciences et de techniques différentes est tel que nous avons sélectionné pour notre étude uniquement celles qui sont fréquemment usitées et dont l'utilisation en procédure pénale n'est pas prohibée.

13 Enfin, dans la troisième partie, nous répondrons aux deux ultimes questions et émettrons des propositions en conséquence.

PREMIERE PARTIE: LE CONTEXTE HISTORIQUE ET JURIDIQUE

CHAPITRE 1: LES DÉFINITIONS GÉNÉRALES ET L'ÉVOLUTION HISTORIQUE

I. Les définitions générales

14 Les expressions *procédure pénale* (A.), *preuve* (B.) et *nouvelles technologies* (C.) sont au centre de notre étude. Ces notions doivent donc être définies.

A. La procédure pénale

15 L'intérêt à la sécurité publique commande que l'auteur d'une infraction réprimée par la loi soit condamné – en principe – par une autorité judiciaire[1].

16 La procédure pénale est la mise en œuvre du droit pénal qui comprend deux aspects[2]: l'aspect organique – concernant l'organisation des juridictions et leurs compétences –, et l'aspect fonctionnel – définissant les phases procédurales (préliminaire, préparatoire et judiciaire). Plus précisément, elle se définit comme "*l'ensemble des règles qui déterminent l'organisation, la compétence et le fonctionnement des autorités judiciaires qui concourent à la répression des infractions et définissent la marche à suivre et les formalités à respecter pour la constatation, l'instruction et le jugement des infractions*"[3].

17 L'idéal procédural peut être approché lorsque les règles édictées tendent à la recherche de la vérité dans le droit et par le droit tout en respectant l'intérêt de l'individu qui doit bénéficier d'un jugement impartial et honnête de sa culpabilité[4].

---

[1] JOSITSCH, Strafprozessrechts, p. 1-2; PIQUEREZ, Traité de procédure pénale suisse, p. 3; RASSAT, p. 11-12; RIEDO, FIOLKA, NIGGLI, p. 4; SCHMID, Handbuch, p. 1-2.

[2] AESCHLIMANN, p. 3-6; GARRAUD, T. I, p. 3; LAINGUI, LEBIGRE, T. II, p. 11; PIQUEREZ, Traité de procédure pénale suisse, p. 5; RASSAT, p. 11; RIEDO, FIOLKA, NIGGLI, p. 4.

[3] PIQUEREZ, Traité de procédure pénale suisse, p. 4.

[4] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 7-8; EICKER, HUBER, p. 5; GARRAUD, T. I, p. 4-5; SCHMID, Handbuch, p. 3-4.

B. La preuve

18 Aristote emploie le terme *πίστίσ* traduisible par foi ou croyance, Cicéron emploie la racine latine *probatio* qui désigne le moyen de persuader et Quintilien utilise les termes *signa*, *argumenta*, *exempla*. L'emploi de mots divers et variés nous démontre qu'il est impossible d'admettre une définition unique de la *preuve*.

19 Etymologiquement, le mot *preuve* a pour racine le verbe latin *probare* qui signifie "*estimer bon*", "*approuver*", "*faire approuver*", "*rendre croyable*" ou "*prouver*"[5].

20 En procédure pénale, la preuve intervient du soupçon de commission à la décision. Par exemple, l'ouverture d'une instruction est ordonnée "*lorsqu'il ressort du rapport de police, des dénonciations ou [des] propres constatations [du ministère public] des soupçons suffisants*" (art. 309 al. 1 let. a CPP[6]). L'article 7 CPP dispose que "*[l]es autorités pénales sont tenues [...] d'ouvrir et de conduire une procédure lorsqu'elles ont connaissance [...] d'indices permettant de présumer l'existence d'infractions.*". L'acte d'accusation est rédigé "*lorsque [le ministère public] considère que les soupçons établis sur la base de l'instruction sont suffisants [...]*" (art. 324 al. 1 CPP). Au stade de l'enquête et de l'instruction, le législateur emploie les termes *soupçons* ou *indices* explicitant l'idée d'un fait vraisemblable, mais sans être donné pour certain[7]. Au stade du jugement, "*le tribunal apprécie librement les preuves recueillies selon l'intime conviction qu'il tire de l'ensemble de la procédure.*" (art. 10 al. 2 CPP), le juge doit interpréter les soupçons et les indices recueillis pour atteindre un certain degré de certitude. Le législateur transpose alors le mot *preuve* aux notions de *soupçons* ou d'*indices*.

21 En droit, la preuve est donc l'activité déployée lors d'un procès pour démontrer l'existence ou l'inexistence d'un fait ou la production d'éléments pour convaincre le juge de l'existence ou de l'inexistence d'un fait et/ou pour identifier un auteur. Elle a pour objet les moyens de démonstration et comme fonction de forger l'intime conviction[8].

22 La preuve pénale peut donc permettre d'élucider des infractions et de punir les criminels, ou de faire subsister un doute et donc de permettre d'acquitter.

---

[5] BRACHET Jean-Paul, MOUSSY Claude, *Latin et langues techniques*, Paris 2006, p. 171-173.

[6] Code de procédure pénale suisse (CPP) du 5 octobre 2007, RS 312.00.

[7] GALLUSER, p. 2; PIQUEREZ, Traité de procédure pénale suisse, p. 325.

[8] BÉNÉDICT, p. 29; CORNU Gérard, *Vocabulaire juridique*, 8ème éd., Paris 2007, p. 358; GALLUSER, p. 1; GARRAUD, T. I, p. 9; GILLIÉRON, p. 1; MERLE, VITU, T. II, p. 177; PIQUEREZ, Traité de procédure pénale suisse, p. 324-325; PIQUEREZ, RJJ 2004, p. 8.

C. Les nouvelles technologies

23 L'expression *nouvelles technologies* concerne les divers domaines évolutifs de la technologie. Aucune définition précise n'existe sur le sujet, il nous faut donc en créer une.

24 La *technologie* provient du grec *τεχνολογία*. Le premier élément *τέχνη* signifie "*art*" ou "*artifice*" et le second *λογία* désigne la "*description précise d'un phénomène*"[9]. En regroupant ces éléments, nous pouvons en déduire que, lorsque l'on parle d'une technologie, nous "*dissertons sur un art*"[10]. Plus spécifiquement, il s'agit d'un savoir-faire dans un domaine particulier et requérant des connaissances spécifiques.

25 De manière générale, l'expression *nouvelles technologies* est synonyme d'innovation qui, dans la mesure où notre champ d'étude s'étend du domaine médical au domaine informatique en passant par divers domaines techniques, doit être comprise dans un sens large. Elle englobe la biotechnologie (analyse génétique à l'aide de l'ADN), la biométrie (identification grâce aux empreintes digitales), les hautes technologies (téléphonie fixe ou mobile, messagerie électronique, vidéosurveillance et GPS) et les technologies de l'information et de la communication (ordinateur, Internet et bases de données).

26 Relevons encore que ce qui peut être considéré comme *nouvelles technologies* ne le sera plus dans quelques années. Ce terme est donc extrêmement relatif et évolutif. De manière un peu arbitraire, nous emploierons ce terme pour regrouper toutes les sciences et les techniques analysées dans notre travail.

II. L'évolution historique

27 Maints auteurs[11] se sont intéressés à l'histoire de la procédure pénale. Nous exposons dans cette partie l'historique des procédures accusatoire, inquisitoire et mixte (A.) et leurs influences sur la preuve, puis l'historique des nouvelles technologies (B.).

---

[9] CHARPIN, Solaris n° 4.

[10] DICTIONNAIRE ETYMOLOGIQUE DU FRANÇAIS, *technique – technologie,* Paris 2009; DICTIONNAIRE ETYMOLOGIQUE ET HISTORIQUE DU FRANÇAIS, *technique – technologie,* Paris 2007.

[11] CARBASSE, Histoire du droit pénal et de la justice criminelle; FRANCHIMONT, JACOBS, MASSET, p. 20-31; HAUSER, SCHWERI, HARTMANN, p. 10-14; LAINGUI, LEBIGRE, T. II; MERLE, VITU, T. I, p.169-186; PIQUEREZ, Traité de procédure pénale suisse, p. 40-56; RASSAT, p. 29-42; SCHMID, Strafprozessrecht, p. 50-53.

A. Les procédures accusatoire, inquisitoire, mixte et l'administration de la preuve

> *"Chaque âge reflète visiblement dans la procédure criminelle qui le caractérise, la foi fondamentale qui l'anime, c'est-à-dire sa croyance la plus universelle et la plus indiscutée. En sorte que la série des transformations législatives et judiciaires sur ce point correspond aux transformations mêmes de la pensée humaine." (Gabriel TARDE)*[12]

28 Gabriel Tarde fonde sa théorie de la société, notamment judiciaire, sur les liens sociaux qui assurent la cohésion et la sécurité collective. Conformément à cette pensée, la société et la morale influent sur la justice, c'est pourquoi elle évolue au gré des années et des courants de civilisation. L'évolution des systèmes procéduraux et de l'administration de la preuve pénale ne déroge pas à cette théorie sociale[13].

29 La plupart des Etats ont débuté avec une procédure accusatoire (1.), puis ont glissé dans une procédure inquisitoire (2.). Depuis la Révolution française, le système mixte s'est mis en place (3.). Le passage d'un système à l'autre a influencé l'administration de la preuve, plus spécifiquement les moyens de preuves.

30 De tout temps, la collectivité a été désireuse de rendre la justice avec le moins d'erreur possible. Pour obtenir la vérité, la société n'a jamais cessé de rechercher le moyen de preuve par excellence et, pour le découvrir, elle a procédé par tâtonnement. La transformation de la preuve pénale n'est donc que le reflet de la pensée humaine et, par conséquent, de l'évolution de la procédure pénale[14].

---

[12] Gabriel TARDE dans GILLIERON, p. 2.

[13] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 23-25 et 29 ss; FRANCHIMONT, JACOBS, MASSET, p. 21; GARRAUD, T. I, p. 10 ss; LAINGUI, LEBIGRE, T. II, p. 34-49.

[14] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 180 ss; CARBASSE, Introduction historique au droit pénal, p. 136-141; FRANCHIMONT, JACOBS, MASSET, p. 1018-1020; GARRAUD, T. I, p. 497-500; GILLIERON, p. 5-12; LAINGUI, LEBIGRE, p. 24-27 et 110-121; LECLERC H., p. 206-211; MERLE, VITU, T. I, p. 170-186; PIQUEREZ, Traité de procédure pénale suisse, p. 328-330.

1. Le système accusatoire

a. Les principes généraux

31 Le droit romain primitif et le haut Moyen-Âge ont une procédure accusatoire[15]. Ce système est donc historiquement le premier.

32 Le système accusatoire trouve sa racine terminologique dans le déroulement de la procédure qui débute après une accusation[16]. Il instaure une large participation des citoyens à la justice et se compose de trois traits caractéristiques: le débat, le rôle du juge et la recherche de la vérité[17].

33 Grâce à une procédure orale, publique et contradictoire, le système accusatoire garantit l'impartialité du décideur, la contradiction des débats, le principe de publicité et l'égalité des armes[18]. Ce régime procédural se centre sur l'intérêt de l'accusé à pouvoir bénéficier d'un jugement réfléchi et juste.

34 En revanche, l'Etat n'a pas la compétence d'agir d'office[19]. Seul un particulier peut mettre en mouvement la poursuite grâce à une accusation. A défaut d'accusateur, le crime ou le délit reste impuni: "*Nocens, nisi accusatus fuerti, condemnari non potest*"[20], ce qui crée un réel danger pour la sécurité publique. De plus, les débats tenus par les parties ne se concentrent souvent pas sur les points essentiels de l'affaire et l'administration de la preuve. Faute de pouvoir investiguer et obtenir des informations complémentaires, le juge doute et ne peut qu'acquitter l'accusé.

b. L'administration de la preuve en procédure accusatoire

35 Le rôle du juge – un citoyen choisi ou accepté par les parties[21] – est uniquement d'arbitrer la confrontation entre l'accusé et l'accusateur. Il doit rester impartial et passif. Il veille uniquement au respect par les parties des exigences découlant de la loi ou de la coutume lors de l'administration probatoire. Les débats terminés, le juge se demande si la culpabilité de

---

[15] FRANCHIMONT, JACOBS, MASSET, p. 21; GARRAUD, T. I, p. 15-16; MERLE, VITU, T. I, p. 169.

[16] RASSAT, p. 29 et 42.

[17] GARRAUD, T. I, p. 11; PIQUEREZ, Traité de procédure pénale suisse, p. 40-41.

[18] GARRAUD, T. I, p. 14; JEANNERET, KÜHN, p. 48; LAINGUI, LEBIGRE, p. 24 et 35; MERLE, VITU, T. I, p. 169.

[19] MERLE, VITU, T. I, p. 170; PIQUEREZ, Traité de procédure pénale suisse, p. 42.

[20] CICERON cité dans CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 40.

[21] A ce sujet: GARRAUD, T. I, p. 13; RASSAT, p. 30; SCHMID, Handbuch, p. 73.

l'accusé est suffisamment établie. Il recherche la vérité procédurale, c'est-à-dire une vérité relative qui se dégage de la procédure contradictoire.

36 Ne connaissant pas la loi, le juge se réfère aux us, aux coutumes et aux "*puissances supérieures dont [il est] le jouet et bien souvent l[a] victime*" pour rendre un verdict[22].

37 En procédure accusatoire, l'administration de la preuve n'est pas toujours obligatoire. En cas de flagrant délit ou d'aveu de l'accusé, l'accusateur est dispensé de produire des preuves et le juge fixe simplement la peine[23]. A défaut, le juge laisse le soin aux divinités ou aux forces mystérieuses de désigner sans erreur le coupable.

38 Trois moyens de preuves sont connus et administrés par les parties: les ordalies, le serment purgatoire et le duel judiciaire.

39 Les ordalies ou jugements de Dieu se fondent sur la morale religieuse d'après laquelle un innocent est confronté à des dommages sérieux – épreuve de l'eau ou de l'huile bouillante et ordalie du fer rouge destinée à voir si une lésion corporelle se soigne ou non, ordalie de l'eau froide consistant à plonger l'accusé pieds et poings liés dans l'eau et voir s'il se noie, etc.[24] –, les divinités prendront parties à l'administration de la justice[25]. Ces moyens de preuves permettent de constater soit la pureté, soit l'impureté des accusés[26]. Il ne s'agit donc pas de savoir si les faits sont vrais.

40 Les forces mystiques peuvent également déterminer le coupable. Par exemple, le sens de la fumée provenant d'un bûcher indique au juge dans quelle direction se trouve le coupable, ou encore, l'épreuve du cercueil confronte l'accusé au cadavre et si une modification intervient sur celui-ci alors la culpabilité est confirmée.

41 Le serment purgatoire prend Dieu à partie car celui qui ment devant lui risque la damnation. L'accusé jure de son innocence sur l'Evangile et des cojureurs affirment l'honnêteté de celui-là[27].

---

[22] Henry LEVY-BRUHL dans FRANCHIMONT, JACOBS, MASSET, p. 1019.

[23] GARRAUD, T. I, p. 498.

[24] A ce sujet, voir: CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 92-97; FRANCHIMONT, JACOBS, MASSET, p. 1019; LAINGUI, LEBIGRE, p. 24-27.

[25] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 95-96; CARBASSE, Introduction historique au droit pénal, p. 72-74; GARRAUD, T. I, p. 499; GILLIERON, p. 5-6; LAINGUI, LEBIGRE, p. 26; PIQUEREZ, Traité de procédure pénale suisse, p. 329.

[26] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 94.

[27] CARBASSE, Introduction historique au droit pénal, p. 71; LAINGUI, LEBIGRE, p. 25-26.

42 Quant au duel judiciaire, considéré comme une ordalie bilatérale, il consiste en l'affrontement des deux parties dans un combat singulier[28]. Dieu ou ses anges se tiennent à côté du juste qui l'emporte.

43 Suite à ces épreuves qui instaurent le principe de la présomption de culpabilité, le juge rend son verdict sans crainte. En effet, les incertitudes sont dissipées par le jugement de Dieu et la volonté des puissances mystiques déchargeant le juge de toute responsabilité[29].

2. Le système inquisitoire

a. Les principes généraux

44 A l'exception de la Grande-Bretagne, le système inquisitoire est mis en place dans les pays d'Europe au détriment du système accusatoire[30].

45 Son avènement s'explique par une triple volonté: réprimer les infractions d'office en appliquant l'adage "[*t*]*out juge est procureur général*", professionnaliser la fonction de magistrat et rechercher la vérité matérielle.

46 Les actes délictuels ne sont plus reconnus comme exclusivement préjudiciables à la victime ou à sa famille, ils troublent la collectivité en ébranlant la sécurité publique[31]. Le magistrat – représentant de l'Etat et professionnel – procède d'office à la poursuite des infractions et a le devoir de rechercher activement les preuves pour découvrir la vérité[32]. Il n'est pas autorisé à fonder sa décision sur sa subjectivité et ne peut condamner à une peine entière qu'en présence d'une *probatio plena* – preuve pleine – ou de plusieurs *probatio semiplenae* - semi-preuves[33]. Selon le Digeste: "*Il vaut mieux laisser un coupable impuni plutôt que de condamner un innocent*"[34]. Nous pouvons y voir l'apparition du principe de la présomption d'innocence[35].

---

[28] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 96-97; CARBASSE, Introduction historique au droit pénal, p. 74-75.

[29] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 94; GILLIÉRON, p. 5.

[30] CARBASSE, Introduction historique au droit pénal, p. 132; FRANCHIMONT, JACOBS, MASSET, p. 22; GARRAUD, T. I, p. 16; HAUSER, SCHWERI, HARTMANN, p. 11-12; LAINGUI, LEBIGRE, p. 47; RASSAT, p. 33-34.

[31] FRANCHIMONT, JACOBS, MASSET, p. 22.

[32] GARRAUD, T. I, p. 16; MERLE, VITU, T. I, p. 177; PIQUEREZ, Traité de procédure pénale suisse, p. 44; RASSAT, p. 34.

[33] A ce sujet, voir: GARRAUD, T. I, p. 503-505; LAINGUI, LEBIGRE, p. 113-116.

[34] Digeste cité dans CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 194; CARBASSE, Introduction historique au droit pénal, p. 139.

[35] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 195; CARBASSE, Introduction historique au droit pénal, p. 139; CHASSAING, n° 11; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 12; GARRAUD, T. I, p. 509.

47 Grâce à l'instruction d'office des affaires et à la professionnalisation des juges, la procédure inquisitoire limite l'impunité des délinquants.

48 En revanche, le caractère écrit, la non-intégration de la victime dans le procès et l'inexistence du débat déshumanisent le procès pénal. En perdant sa qualité de partie, la victime ne peut pas se confronter à l'accusé durant le jugement. Le débat loyal – mettant sur pied d'égalité l'accusateur et l'accusé – est remplacé par les questions incessantes du juge. Preuve incontestée, l'aveu est systématiquement recherché et pour l'obtenir, le recours à la torture est fréquent[36]. Couplé à l'absence de défense, la torture engendre l'arbitraire dans le procès pénal.

b. L'administration de la preuve en procédure inquisitoire

49 Sous l'égide de la procédure inquisitoire, les moyens de preuves admissibles et leur force probante sont enracinés dans la loi. Deux modes probatoires principaux sont réglementés: le témoignage et l'aveu[37].

50 Concernant le témoignage, la loi règle quelques principes fondamentaux: le témoin doit être idoine, le témoignage d'un homme vaut celui de deux femmes et les témoignages des moins de 14 ans ou des vils sont irrecevables[38]. Lorsque deux témoins énoncent des faits similaires, la preuve est pleine et suffit; lorsqu'il n'existe qu'un seul témoin, le juge bénéficie d'une *probatio semiplenae*[39]. Le présumé délinquant peut alors démentir les faits ou les avouer.

51 Lorsque les dires des témoins laissent paraître que l'accusé ment en niant l'évidence ou si seule une *probatio semiplenae* est apportée, le juge doit forger son intime conviction et pour ce faire, il a besoin de l'aveu de l'accusé.

52 Progressivement, pour éviter l'administration fastidieuse des preuves, le recours à l'aveu considéré comme la *probatio probatissima* est devenu le but de tout procès pénal afin d'acquérir l'intime conviction[40]. "*C'est pour cela que faute d'autres moyens pour parvenir à cette entière conviction, on s'est vu obligé de torturer le corps de l'accusé.*"[41].

---

[36] AESCHLIMANN, p. 60-61.

[37] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 194-195; GARRAUD, T. I, p. 499; GILLIERON, p. 6; PIQUEREZ, Traité de procédure pénale suisse, p. 329.

[38] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 195; GILLIERON, p. 6; LAINGUI, LEBIGRE, p. 111-112.

[39] FRANCHIMONT, JACOBS, MASSET, p. 1020.

[40] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 200; GILLIÉRON, p. 7; LAINGUI, LEBIGRE, p. 116; PIQUEREZ, Traité de procédure pénale suisse, p. 349-350; ST-YVES-ST-YVES, MEISSNER, p. 155.

53 Peu à peu, les dérives de ce système probatoire ont occulté la présomption d'innocence. Le recours à la torture suggère que l'accusé, en niant les faits, ment et qu'il est d'office considéré comme coupable. Les penseurs du XVIIIe siècle commencent à douter de la force probante de cette preuve dont l'effet est incertain et mène à l'arbitraire[42]. Un délinquant endurci et physiquement fort niant sous la torture est acquitté, alors qu'un innocent faible de caractère et de carrure peut avouer un crime qu'il n'a pas commis.

3. Le système mixte

a. Les principes généraux

54 En réponse aux excès du système inquisitoire, les philosophes, écrivains et professionnels du droit ont désiré humaniser la procédure pénale en abolissant la torture et en luttant contre la peine de mort[43]. Le retour au système accusatoire n'étant pas souhaitable, la plupart des Etats européens occidentaux ont mis en place le système mixte[44]. Depuis le XVIIIe siècle, ce dernier n'a cessé d'évoluer.

55 Dès 1830, la création du ministère public, l'extension des droits de la défense, l'introduction des principes de publicité, d'oralité, d'immédiateté et l'administration de la preuve concrétisent l'humanisation du procès pénal, tout en luttant contre la criminalité[45]. La fin du XIXe et le milieu du XXe siècle signent la dernière amélioration historique du régime mixte[46]. Le progrès des innovations techniques et scientifiques (photographie, vidéosurveillance, empreinte génétique, dactyloscopie, donnée électronique) permettent une meilleure efficacité dans l'administration de la preuve et la découverte de la vérité. Parallèlement, en 1948, les droits de l'accusé se renforcent grâce à la Convention européenne des droits de l'Homme[47] – relais des principes accusatoires – qui instaure notamment le droit à la liberté et à la sûreté (art. 5 CEDH) et le droit à un procès équitable (art. 6 CEDH).

---

[41] Muyard de VOUGLANS cité dans LECLERC H., p. 208.

[42] FRANCHIMONT, JACOBS, MASSET, p. 1020 citent BECCARIA, MONTESQUIEU, VOLTAIRE.

[43] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 390-399; ENCYCLOPEDIE UNIVERSALIS, *Bentham*, 6ème éd., Paris 2008, Tome 3; ENCYCLOPEDIE UNIVERSALIS, *Lumières (Philosophie des)*, 6ème éd., Paris 2008, Tome 14; GARRAUD, T. I, p. 63-64; LAINGUI, LEBIGRE, p. 127-130; PIETH, p. 27.

[44] A ce sujet: CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 16, 123-124 et 389-392.

[45] HAUSER, SCHWERI, HARTMANN, p. 13.

[46] PIQUEREZ, Traité de procédure pénale suisse, p. 49-50.

[47] Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), RS 0.101.

56 Le système mixte correspond à une procédure pénale qui combine les garanties et les qualités du système accusatoire et du système inquisitoire. Contrairement aux deux précédents systèmes procéduraux, il est difficile d'extraire de ce régime les traits principaux de manière tangible[48].

57 En procédure mixte, la saisine appartient à la victime et aux fonctionnaires spécifiques – ministère public ou juges d'instruction selon les modèles – chargés de veiller au bien de la collectivité lorsqu'un acte délictuel leur est rapporté[49]. La décision appartient aux magistrats professionnels pouvant être assistés ou aidés de non-professionnels appelés jurés qui recherchent la vérité matérielle en appréciant librement la force probante des preuves[50].

58 En Suisse, la procédure pénale fédérale est issue du système mixte empreint des garanties accusatoires. En adoptant le modèle "ministère public II"[51], un unique organe a la compétence d'enquêter, de poursuivre et d'instruire. La procédure pénale débute avec un avant-procès scindé en une phase préliminaire (l'enquête) et une phase dite préparatoire (l'instruction), et se poursuit avec la phase des débats (le jugement).

59 L'avant-procès avec la recherche des preuves est secret, écrit, peu ou pas contradictoire, les deux phases le constituant sont inquisitoires. Néanmoins, quelques décisions – comme la mise en détention provisoire (art. 18 al. 1 CPP) – requièrent un débat contradictoire devant le Tribunal des mesures de contraintes[52].

60 Le procès composé très largement d'échanges d'arguments ou d'explications devant un tribunal public, se déroulant oralement et de manière contradictoire, la phase des débats découle du système accusatoire[53].

61 Après la clôture de l'instruction, si le ministère public considère que les soupçons établis sur la base de l'instruction démontrent la culpabilité vraisemblable de l'auteur, il renvoie le prévenu devant la juridiction compétente pour jugement (art. 324 ss CPP). Sinon, il prononce le classement (art. 319 ss CPP). En cas de renvoi en jugement, l'accusation est soutenue par le ministère public.

---

[48] GARRAUD, T. I, p. 21; LAINGUI, LEBIGRE, p. 137-138; MERLE, VITU, T. I, p. 185; RASSAT, p. 35-36.

[49] JOSITSCH, Strafprozessrechts, p. 17-18; PIETH, p. 38-39; Polizeiliche Ermittlung-VOSER, p. 28-29; SCHMID, Handbuch, p. 60-73; SCHMID, Praxiskommentar, art. 7 N 1-3.

[50] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 14;GARRAUD, T. I, p. 21; MERLE, VITU, T. I, p. 186.

[51] De 29 à l'unité, p. 33; Rapport explicatif relatif à l'avant-projet, p. 18; RIEDO, FIOLKA, NIGGLI, p. 44.

[52] CR-CPP-LOGOS, art. 225 N 4; SCHMID, Praxiskommentar, art. 225 N 2.

[53] GARRAUD, T. I, p. 21; JOSITSCH, Strafprozessrechts, p. 31; RASSAT, p. 37; SCHMID, Handbuch, p. 110-113; SCHMID, Praxiskommentar, art. 66 N 1-3 et art. 69 N 1-4.

62 Si l'ensemble de la procédure est conduit par une unique autorité pénale, l'objectivité, l'indépendance et le respect des garanties de l'Etat de droit peuvent être mis à mal. C'est pourquoi, pour contrebalancer ces pouvoirs, le Code de procédure pénale renforce les garanties de la défense (par exemple art. 125-136 CPP) et instaure une autorité judicaire indépendante de recours contre toutes les décisions du ministère public (art. 20 CPP).

b. L'administration de la preuve en procédure mixte

63 Les preuves morales du système procédural mixte reposent sur un contexte social qui instaure une justice publique où la conviction de culpabilité dépend uniquement de la conscience du jury populaire ou de celle du magistrat.

64 Pour juger, "il ne faut que le simple bon sens, et ce guide est moins trompeur que tout le savoir d'un juge accoutumé à ne rechercher partout que des coupables et à tout ramener à un système qu'il sait d'après ses études"[54]. C'est pourquoi la valeur d'une preuve ne doit pas être tarifée à l'avance. En d'autres termes, le système mixte voit naître le principe de libre appréciation des preuves et de liberté de la preuve[55].

65 Ainsi, le jugement de culpabilité est rendu en pleine âme et conscience du décideur après que le juge ou les jurés aient acquis l'intime conviction en interprétant les preuves[56].

66 Avec le développement technologique, la phase morale a évolué en phase dite scientifique. L'informatique, les enregistrements audio ou vidéo, ainsi que le développement des preuves formelles dites scientifiques reposant sur les sciences criminalistiques – médico-légal, anthropométrie, toxicologie, dactyloscopie et empreinte génétique[57] – sont autant de moyens de preuves utiles au juge pour former son intime conviction.

67 La complexité de ces moyens probatoires a en outre placé le rapport d'expertise, extensivement l'expert, au centre du procès pénal[58].

---

[54] Beccaria cité dans LECLERC H., p. 208.

[55] Infra Partie I, Chapitre 3, III, B et C; n° 291 ss et 313 ss.

[56] CARBASSE, Histoire du droit pénal et de la justice criminelle, p. 413-419; GARRAUD, T. I, p. 499.

[57] MOUSTIERS, p. 165.

[58] GARRAUD, T. I, p. 500; GILLIERON, p. 10-11; LECLERC H., p. 212; PIQUEREZ, Traité de procédure pénale suisse, p. 380-391. Infra Partie II, Chapitre 1, n° 385-387 et 490 ss.

B. Les nouvelles technologies

68 Avant d'appréhender la place des nouvelles technologies dans le monde judiciaire et leur valeur probante, un aperçu de leur évolution historique permet de déterminer les recherches effectuées, les connaissances acquises et les répercussions sur notre vie quotidienne. En faisant un point de situation et en distinguant la connaissance établie de l'ignorance ou de l'incertitude, nous pourrons objectiver notre jugement sur la force probatoire d'une preuve relevant des nouvelles technologies.

1. La dactyloscopie

a. La découverte des empreintes papillaires

69 L'étude scientifique des empreintes digitales appelée la dactyloscopie débute avec les travaux de Nehemiah Grew – en 1684 – et Marcello Malpighi – en 1686 – qui s'intéressent à l'anatomie de la main, des doigts et des extrémités digitales[59].

70 En 1823, le physiologiste tchèque Jan Evangelista Purkinje publie une thèse sur la variation des dessins papillaires[60]. Il les classifie en neuf types d'empreintes sans entrevoir la possibilité de les utiliser comme moyen identificatoire. Cette classification fait partie du *continuum* des dessins papillaires permettant de trier les fiches dactyloscopiques dans les bases de données[61].

b. La dactyloscopie comme moyen d'identification

71 La découverte d'un moyen pérenne propre à caractériser avec exactitude un être humain est une problématique récurrente pour la justice pénale désireuse de confondre les coupables. C'est pourquoi de nombreux scientifiques ont recherché un moyen permettant d'identifier les individus.

72 Alphonse Bertillon – fondateur de la police scientifique française en 1870 – propose l'anthropométrie comme fondement de l'identification. Le Bertillonnage recourt à un ensemble de mesures osseuses et de longueurs – taille, mesures de la tête, longueur du

[59] ENCYCLOPÉDIE UNIVERSALIS, *Police scientifique*, 6ème éd., Paris 2008, Tome 19; DE VELTERE, p. 129.

[60] ENCYCLOPÉDIE UNIVERSALIS, *Police scientifique*, 6ème éd., Paris 2008, Tome 19; DE VELTERE, p. 129.

[61] Infra Partie II, Chapitre 2, I, A, 2, c, i, n° 543 ss.

médius gauche ou de la coudée, etc. – pour caractériser une personne[62]. En 1880, les empreintes digitales sont intégrées au Bertillonnage comme classificateur subsidiaire et, en 1882, comme caractéristique principale[63].

73 A la même époque, le médecin écossais Henry Faulds suggère d'utiliser les dessins digitaux comme moyen d'identification en confrontant une empreinte retrouvée sur les lieux d'une infraction avec une empreinte d'origine connue[64]. Celle-ci est collectée à l'aide d'encre d'imprimerie puis classifiée, celle-là se révèle par diverses poudres qui dessinent les crêtes dermatoglyphes. La méthode de Faulds permet d'identifier aussi bien les récidivistes que les auteurs d'un premier délit.

74 Le britannique William Herschel, fonctionnaire du Civil Service anglo-indien, renforce la théorie d'Henry Faulds en démontrant la pérennité du dessin papillaire à l'aide de ses propres empreintes encrées restées inchangées entre 1860 et 1888[65].

75 Reprenant les travaux d'Henry Faulds et de William Herschel, Francis Galton développe un système de classification rendant les recherches d'identité aisées et affirme les trois prémisses fondamentales de la dactyloscopie à savoir: la pérennité, l'inaltérabilité et l'individualité des dessins papillaires[66]. Corrélativement au système de Jan Evangelista Purkinje, le *continuum* pour le classement dactyloscopique se base sur les travaux de Francis Galton[67].

76 La découverte de Francis Galton accélère l'intégration et l'utilisation des empreintes digitales par les autorités pénales. En 1892, pour la première fois, un crime est résolu à l'aide d'empreintes contenues dans un fichier. En 1901, en collaboration avec Scotland Yard et sous la direction d'Edward Henry, Francis Galton crée le premier fichier dactyloscopique décadactylaire[68]. En 1902, suite à l'arrestation de Henri-Léon Scheffer, les empreintes digitales deviennent l'une des principales preuves lors des enquêtes policières[69]. En 1914, la dactyloscopie s'impose dans toute l'Europe comme unique méthode d'identification[70].

---

[62] BERTILLON, p. 13; ENCYCLOPÉDIE UNIVERSALIS, *Police scientifique*, 6ème éd., Paris 2008, Tome 19.

[63] BERTILLON, p. 17-26; CHAMPOD, Reconnaissance, p. 5.

[64] FAULDS, On the Skin-furrows of the Hand.

[65] HERSCHEL, Skin Furrows of the Hand.

[66] GALTON, p. 10-16 et p. 60-107.

[67] Infra Partie II, Chapitre 2, I, A, 2, c, i, n° 543.

[68] CHAMPOD, Reconnaissance, p. 7; KOZO, p. 66.

[69] BERLIERE Jean-Marc, L'affaire Scheffer: une victoire de la science contre le crime ? , in *Criminocorpus*, Paris 2007, disponible sur : http://www.criminocorpus.cnrs.fr [consulté le 08.05.2016].

[70] CHAMPOD, Reconnaissance, p. 7; DE VELTERE, p. 130.

77 Depuis le début du XXe siècle, les recherches sur la dactyloscopie s'exercent principalement sur le nombre d'empreintes collectées, sur le mode de prélèvement, sur leur conservation et sur l'amélioration des classifications. Aujourd'hui, les empreintes sont photographiées, numérisées et traitées par ordinateur. Des programmes spécifiques les comparent, identifient les similitudes et les différences, puis indiquent une liste d'empreintes pouvant correspondre.

78 Depuis 1984, la Suisse emploie le système automatique d'identification des empreintes digitales AFIS – Automated Fingerprint Identification System – qui permet d'effectuer en quelques minutes une comparaison entre des traces trouvées sur le lieu d'un crime et celles présentes dans le fichier. Grâce à ce système automatisé, il devient possible d'enregistrer directement dans l'ordinateur des empreintes papillaires de manière numérique.

c. Quelques chiffres démontrant l'importance des empreintes papillaires et du fichier AFIS en Suisse

79 Au 31 décembre 2014, la base de données AFIS contient 842'271 dessins papillaires des dix doigts – alors qu'elle en comptait environ 350'000 de moins en 1998 et 767'415 en 2011 – ainsi que 89'908 traces et 33'103 empreintes de deux doigts[71].

80 Ces trois dernières années, une tendance stabilisatrice se dessine quant au nombre de hit – avec toutefois un pique de 10'000 identifications supplémentaires en 2012 avec la méthode des deux doigts – et au nombre d'empreintes récoltées par année. En moyenne, depuis ces cinq dernière années, alors que seulement 36'000 nouveaux profils sont intégrés annuellement, ce n'est pas moins de 52'800 identifications de personnes grâce à la méthode des deux doigts, 22'500 identifications de personnes grâce à la méthode des dix doigts et 2'850 identifications de traces qui sont réalisées[72]. Quotidiennement, cela correspond à l'identification de 214 suspects environ.

81 En une centaine d'années, les recherches sur la dactyloscopie, le développement des modes de collecte et de conservation des dessins digitaux, la croissance des données contenues dans les fichiers dactyloscopiques et les possibilités de hit ont permis aux empreintes papillaires de s'imposer comme méthode d'identification.

[71] Chiffres fournis par les services AFIS ADN de l'Office fédéral de la police (Fedpol).

[72] Chiffres fournis par les services AFIS ADN de l'Office fédéral de la police (Fedpol).

2. L'acide désoxyribonucléique

a. La découverte de la molécule d'acide désoxyribonucléique

82 Le XIX^e^ siècle est marqué par les premières recherches concernant la molécule d'acide désoxyribonucléique abrégée ADN.

83 Au milieu du XIX^e^ siècle, en croisant diverses variétés de pois, Georg Johann Mendel établit l'existence d'une transmission des caractéristiques biologiques des "parents" vers leurs "enfants"[73]. L'histoire de l'ADN étant étroitement liée au développement de la génétique, les travaux de Georg Johann Mendel vont influencer les recherches du XX^e^ siècle visant à définir le rôle de l'ADN.

84 Au début des années 30, des théoriciens s'intéressent à la base moléculaire responsable de la conservation et de la transmission des caractéristiques héréditaires. Quatorze ans plus tard, le médecin et enseignant-chercheur Oswald Theodore Avery, en collaboration avec Colin MacLeod et Maclyn McCarty, démontrent que la molécule d'acide désoxyribonucléique est porteuse des caractéristiques héréditaires des êtres vivants[74]. Le rôle de l'ADN est identifié comme étant un support informatif, mais sa structure moléculaire est encore inconnue.

85 Dans le laboratoire de Cavendish à Cambridge au milieu de l'année 1952, James Dewey Watson et Francis Crick analysent la structure hélicoïdale à triple hélice proposée un an plus tôt par Linus Pauling et constatent que le chimiste et physicien américain a commis une erreur en omettant les liaisons peptidiques. Le 25 avril 1953, ils proposent un modèle hélicoïdal à double hélice[75]. Cette découverte est récompensée par le prix Nobel de physiologie et de médecine.

86 Quelques années plus tard, Francis Crick émet l'hypothèse que les informations génétiques proviennent d'une séquence d'ADN codée et déchiffre le code génétique en 1966[76]. Aujourd'hui, le décryptage du génome humain est officiellement achevé, mais les recherches sur l'ADN se poursuivent pour qu'il dévoile tous ses secrets.

---

[73] MARTY, MONIN, p. 2; MENDEL Johann, Versuche über Pflanzen-Hybriden, in *erhandlungen des naturforschenden Vereines in Brünn* vol. IV (1865) p. 3-47; ROHMER, Thèse, p. 5.

[74] AVERY, MACLEOD, MCCARTY, p. 137-158; MARTY, MONIN, p. 64-73; ROHMER, Thèse, p. 5.

[75] CRICK, WATSON, p. 737-738; MARTY, MONIN, p. 109-112; ROHMER, Thèse, p. 5; RUCKSTUHL, DITTMANN, ARNOLD, p. 543.

[76] WATSON James, *The double helix: a personal account of the discovery of the structure*, Londres 1968.

b. L'ADN comme moyen identificatoire

87 Jusqu'en 1984, un seul cas significatif d'exploitation du profil génétique comme preuve indiciale est à dénombrer. Il s'agit de l'analyse des cendres d'Anna Anderson qui déclarait en 1920 être la grande-duchesse Anastasia Romanov ce que les tests ADN ont permis de nier.

88 A partir de 1984, la découverte par le professeur Alec Jeffreys des minisatellites variables révolutionne le mode d'identification de l'individu. Aidé par l'invention de la technique PCR – *Polymerase Chain Reaction*[77] – de Kary Mullis, Alec Jeffreys crée deux ans plus tard le profil génétique à l'aide du protocole d'identification nommé "*polymorphisme de longueur des fragments de restriction*"[78].

89 Les analyses ADN deviennent alors un moyen d'investigation judiciaire permettant d'identifier formellement les criminels et s'intègrent dans la procédure pénale. La technique d'Alec Jeffreys est utilisée pour la première fois par un tribunal de Pennsylvanie en 1986[79]. Un an plus tard, Colin Pitchfork, un ouvrier boulanger anglais est confondu par une analyse ADN comme étant l'assassin de deux jeunes filles[80]. 1987 est également l'année de la première condamnation aux Etats-Unis d'un violeur, Tommy Lee Andrews, identifié par son profil génétique[81]. Au mois d'août 1988, la France procède à son premier test ADN dans une affaire de viol. Ce même mois, Zurich utilise dans son institut de médecine légale l'analyse ADN dans un premier temps lors des recherches en paternité, puis dans des cas de viols[82]. L'année suivante, Gary Dotson a été le premier suspect innocenté à l'aide du test ADN[83].

90 Après avoir plébiscité durant huit années l'exploitation du profil génétique comme moyen d'investigation judiciaire, un doute sur la valeur probatoire de l'ADN a lieu en 1994. La défense d'O.J. Simpson combat vivement les résultats des tests effectués, la procédure désordonnée des experts ayant possiblement contaminé les échantillons. La justice acquitte O.J. Simpson.

---

[77] Infra Partie II, Chapitre 2, II, A, 4, b, n° 832-833.

[78] HUYGHE, ADN, p. 56; MOUSTIER, p. 166; ROHMER, Banques de données ADN, p. 199; ROHMER, Thèse, p. 61-66.

[79] Affaire *Pestinikas c. Etat de Pennsylvanie*, arrêt de décembre 1986, 617 A. 2d 1339-1344.

[80] HUYGHE, ADN, p. 3 et 56-58; Informations disponibles sur le site internet de l'Institut de médecine légale du Royaume-Uni: http://www.forensic.gov.uk [consulté le 23.04.2009] .

[81] HIBBERT, p. 767; HUYGHE, ADN, p. 60.

[82] ROHMER, Thèse, p. 62; Informations disponibles sur le site internet de l'Institut de médecine légale de l'Université de Zurich: http://www.irm.uzh.ch [consulté le 08.05.2016].

[83] DOLDSON Gary, The Rape that wasn't – the nation's first DNA exonération, in *Northwstern Law – Center on wrongful convictions*, disponible sur: http://www.law.northwestern.edu [consulté le 08.05.2016]; HUYGHE, ADN, p. 60.

91 Toutefois, le doute n'exclut pas l'utilisation de l'analyse génétique qui continue de se perfectionner. L'année de l'acquittement d'O.J. Simpson, l'histoire de la médecine légale connaît le premier cas d'utilisation d'un ADN non humain pour identifier un criminel[84]. En 1998, le docteur Richard Schmidt est déclaré coupable de tentative de meurtre suite à la démonstration qu'un lien existait entre la souche virale VIH qu'il a inoculé à sa compagne et l'ADN d'un de ses patients atteint du Sida[85]. L'ADN viral est utilisé pour la première fois comme pièce à conviction. En 2003, quinze ans après le meurtre de Lynette White, de nouveaux tests ADN s'appuyant sur la proximité de l'ADN familial ont permis de confondre le neveu de la victime, Jeffrey Gafoor[86]. Il s'agit de la première affaire connue d'identification d'un criminel à l'aide de la proximité de l'ADN familial. Aujourd'hui, l'analyse d'une faible quantité d'ADN – provenant d'une goutte de sang, d'un minuscule fragment d'épiderme, d'une pellicule, etc. – même dégradé peut suffir à identifier un individu, et l'ADN familial, viral ou animal peut permettre des corrélations entre un suspect et l'auteur de l'infraction.

c. Le fichier CODIS et quelques chiffres sur l'empreinte génétique comme moyen identificatoire

92 Corrélativement aux fichiers dactyloscopiques, avec l'accroissement du nombre d'analyses génétiques et la reconnaissance du potentiel de l'ADN dans la résolution d'affaires criminelles, la méthode de classification manuelle a montré rapidement ses limites.

93 Dès le début des années 1990, les autorités politiques et judiciaires suisses sont informées de la possibilité de coupler les profils d'ADN à l'aide d'une base de données, mais confrontées au scandale des fiches visant la gestion des données personnelles, le projet est abandonné[87].

94 Face à l'absence d'un système fédéral, le 19 février 1997[88], le Conseil d'Etat genevois autorise le Parquet à constituer une base de données informatisée. Genève devient le premier canton à se munir d'un fichier ADN limité aux traces recueillies sur son territoire et destiné aux profils

---

[84] Affaire *Beamish c. R*, arrêt du 22 juin 1999, AD-0693.

[85] Affaire *Richard J. Schmidt c. Etat de Louisiane*, arrêt du 29 juillet 1997, K97-249.

[86] Affaire *Jeffrey Charles Gafoor c. Régina*, arrêt du 4 juillet 2003, non publié; Convicted after 15 years: the prostitute's killer who watched three men go to jail for his crime, in *The Independent* du 5 juillet 2003.

[87] CEP, 1989, p. 775 ss; GIROD, MARGOT, RIBAUX, WALSH, p. 132.

[88] Arrêté du Conseil d'Etat genevois du 19 février 1997 concernant la création par le Ministère public du canton de Genève d'un fichier informatisé des personnes suspectées de crimes ou délits (principalement à caractère sexuel) et ayant fait l'objet d'analyses portant sur le profil génétique.

génétiques des personnes soupçonnées de crime ou de délit, principalement à caractère sexuel[89].

95 Sur le plan fédéral, une ordonnance est adoptée le 31 mai 2000[90] permettant l'emploi temporaire d'une base de données fédérale. En juillet 2000, la banque de données sur les profils d'ADN, appelée CODIS – Combined DNA Index System – est mise en œuvre pour une période d'essai limitée au 31 décembre 2004. Le 1er janvier 2005, la loi sur les profils d'ADN et l'ordonnance[91] s'y référant entrent en vigueur permettant l'exploitation définitive de CODIS.

96 Ces dernières années, les systèmes informatisés de stockage et de croisement d'empreintes génétiques se sont révélés des outils précieux. Dans CODIS, le nombre de profils a été multiplié par nonante-et-un entre l'année 2000 et l'année 2014 passant de 1'854 à 169'317 profils. Les profils relatifs aux traces retrouvées sur les lieux d'un crime ont considérablement augmenté, étant en 2014 à 56'687. En une année – de 2010 à 2011 –, environ 10'000 nouveaux profils ont été intégrés à la base de données CODIS. Durant ce même laps de temps, 6'322 concordances ont pu être établies entre des traces et des personnes – jouant un rôle, notamment, dans les cas: d'un vol sur cent, d'une séquestration sur cent, d'une lésion corporelle sur quatre-vingts, d'un brigandage sur vingt et surtout dans un cinquième des infractions contre la vie –, et 1'631 concordances entre des traces[92].

97 Les chiffres illustrent l'utilisation toujours plus fréquente de la génétique comme méthode d'investigations criminelles, extensivement comme moyen de preuve. La contribution des empreintes génétiques est aujourd'hui un aspect essentiel de la procédure pénale afin d'identifier les auteurs d'infractions.

---

[89] RECHSTEINER Urs, RION René, *Entreposage des preuves à caractère génétique*, Genève 2003.

[90] Ordonnance fédérale du 31 mai 2000 sur le système d'information fondé sur les profils d'ADN (Ordonnance ADN), RO 2000 1715.

[91] Loi fédérale du 20 juin 2003 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (Loi sur les profils d'ADN), RS 363; Ordonnance fédérale du 3 décembre 2004 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (Ordonnance sur les profils d'ADN), RS 363.1.

[92] Chiffres disponibles sur le site internet du DFJP: http://www.ejpd.admin.ch [consulté le 08.05.2016].

3. Les moyens de télécommunication

a. La découverte de la téléphonie et son évolution

98 Le mot télécommunication est employé pour la première fois en 1904 par Edouard Estaunié dans son Traité pratique de télécommunication électrique[93]. Ce terme définit "toute transmission, émission et réception à distance, de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toutes natures, par fil électrique, radioélectricité, optique ou autres systèmes électromagnétiques"[94]. Autrement énoncé, la télécommunication est un échange d'informations véhiculées par un support. Elle a un rôle unificateur en permettant à la communauté mondiale de se joindre à tout moment et en tout lieu.

99 Depuis l'invention du télégraphe de Chappe, puis du télégraphe électrique[95], la communication électronique a vécu un essor considérable: création du téléphone fixe (*i.*), développement de la téléphonie mobile (*ii.*) et création de la téléphonie VoIP (*iii.*).

i. La découverte de la téléphonie fixe

100 La transmission de la parole était un souhait inné de l'homme. Avec la découverte au XIXe siècle des phénomènes et des lois de l'électromagnétisme, la possibilité de transmettre et de reproduire la voix à distance se concrétise[96].

101 Alexander Graham Bell réalise et présente le 14 février 1876 le premier téléphone permettant de transmettre la parole à l'aide d'une ligne électrique de trois kilomètres[97]. Un an plus tard, le premier central téléphonique est inauguré dans le Connecticut permettant de desservir vingt-et-un abonnés[98]. Malgré les premiers engouements, les réseaux téléphoniques se créent, mais demandent du temps pour être fonctionnels. En outre, le délai d'attente, la connexion hasardeuse et l'indiscrétion possible sont autant de désavantages n'incitant pas les personnes à utiliser ce mode de communication.

102 Ce n'est qu'au début du XXe siècle que l'évolution et l'intégration de la téléphonie fixe s'accélère. En 1920, le Gouvernement suisse crée les PTT – Postes, Téléphones et Télégraphes

---

[93] ESTAUNIE Edouard, *Traité pratique de télécommunication électrique (télégraphie-téléphonie)*, Paris 1904.

[94] Définition provenant de l'Annexe 2 de la Convention internationale des télécommunications du 6 novembre 1982 (entrée en vigueur en Suisse, le 1er avril 1985), RS 0.784.16.

[95] MONTAGNE, p. 125 ss; UIT, p. 3.

[96] ENCYCLOPEDIE UNIVERSALIS, *Télécommunication*, 6ème éd., Paris 2008, Tome 23; MONTAGNE, p. 212-213.

[97] BARDIN, p. 98; MONTAGNE, p. 215-216; UIT, p. 5.

[98] UIT, p. 5.

– pour diriger le réseau téléphonique. Après deux années, l'entreprise met en œuvre à Zurich-Hottingen le premier réseau régional semi-automatique. Puis, en 1936, les PTT installent le premier poste téléphonique public permettant aux non-abonnés de communiquer. En 1948, un demi-million de suisses possèdent un téléphone, et, en 1956, il devient possible de joindre l'Amérique du Nord[99].

103 La croissance du téléphone en Suisse est l'une des plus exponentielles au monde[100]. La Confédération devient même en 1959, la première à se doter d'un réseau téléphonique entièrement automatisé. Puis, en 1988, avec plus de 3 millions d'abonnés, la Suisse s'empare de l'ère du numérique avec la technologie ISDN. Le téléphone se transforme en ligne à grande vitesse pour le son, le texte et les images[101].

104 Avec un taux de pénétration de 61,15 pour cent habitants suisses, la téléphonie fixe a connu son point culminant en 1995[102]. De 1996 à 2013, une perte d'environ 18% d'abonnés est recensée, s'expliquant par l'avènement de la téléphonie mobile[103].

ii. La téléphonie mobile

105 Dès les années 90, grâce au standard GSM – Global System for Mobile communication – la technologie mobile se diffuse avec la mise en service du réseau Natel D réseau de téléphonie mobile numérique et cellulaire, la miniaturisation des appareils et la diminution de leur coût d'achat[104]. N'étant plus réservé à l'usage professionnel ou à l'élite sociale, le téléphone portable supplée dans bon nombre de pays industrialisés le téléphone fixe.

106 Moins de dix années ont suffi pour que le nombre d'utilisateurs soit quintuplé dans le monde, passant de 1,30 milliard d'abonnés en 1997 à 6,954 milliards d'utilisateurs fin 2014[105]. Le taux de pénétration mondial de la téléphonie mobile s'élève en fin 2014 à 96.1%. Dans un pays industrialisé comme la Suisse, l'émergence du réseau mobile est notablement plus significative. De 1990 à 1999, le marché de la téléphonie mobile a évolué de manière

[99] DANESI Marco, L'appel de l'histoire, in *Domaine Public* n° 1671 (2005); Informations disponibles sur le site internet de Swisscom: http://www.swisscom.com [consulté le 10.10.2009].

[100] BOVET, p. 692 et 706.

[101] BARDIN, p. 98; MONTAGNE, p. 215-216; UIT, p. 5.

[102] OFCOM, *Statistique officielle des télécommunications 2011 – Résultat provisoire*, Bienne 2012, p. 11; OFS, *Annuaire statistique de la Suisse 2012*, Zurich 2012, p. 387.

[103] Informations disponibles sur le site de l'OFCOM: http://www.bakom.admin.ch [consulté le 08.05.2016].

[104] Informations disponibles sur le site internet de Swisscom: http://www.swisscom.com [consulté le 10.10.2009].

[105] Informations disponibles sur le site de l'UIT: http://www.itu.int [consulté le 08.05.2016].

exponentielle[106], il s'est stabilisé de 2000 à 2004 et son taux se rehausse à nouveau depuis 2005. Avec plus de 10 millions d'abonnements répertoriés en Suisse durant l'année 2013, on dénombre environ 127 abonnements à la téléphonie mobile pour cent habitants[107]. Chaque Suisse a donc – au moins – un téléphone portable.

107 Parallèlement à la création du standard GSM, le protocole Short Message System plus connu sous le sigle SMS fait son apparition. A partir de 2002, la version améliorée du SMS nommée MMS – Multimedia Messaging Service – permet de transmettre des messages plus longs accompagnés d'images ou de vidéos.

108 En 2013, avec 6'100 milliards de SMS/MMS envoyés dans le monde[108] dont 4,284 milliards depuis la Suisse[109], les SMS/MMS sont devenus un mode et un marché de communication à part entière, même si, suite à l'émergence des applications employant la technologie 3 ou 4G et internet, l'envoi de SMS/MMS est en nette diminution, deux milliards de moins en Suisse depuis 2011.

iii. La téléphonie IP

109 Désirant exploiter les possibilités liées aux moyens informatiques et électroniques, le développement de la communication vocale par réseaux débute en 1996 avec le Netmeeting de l'UIT. N'offrant pas la plupart des fonctions de la téléphonie traditionnelle et coûtant vingt-cinq fois plus cher qu'un poste classique, les premiers systèmes VoIP subissent un échec d'intégration.

110 L'arrivée de l'ADSL, l'augmentation de la rapidité des ordinateurs, la gratuité des systèmes de téléphonie VoIP et le lancement commercial de Skype en 2003 modifient l'utilisation des moyens de télécommunication. Les innovations successives, notamment des fonctionnalités Skype – communication entre deux PC équipés de produit Skype, introduction de la fonction conférence, puis introduction d'un module payant pour appeler un numéro fixe ou être appelé – ont donné l'impulsion nécessaire à la commercialisation grand public de la téléphonie VoIP[110].

---

[106] BOVET, p. 706.

[107] Informations disponibles sur le site de l'OFCOM: http://www.bakom.admin.ch [consulté le 08.05.2016].

[108] Chiffre disponible sur le site internet de Portio Research Ltd: http://www.portioresearch.com [consulté le 08.05.2016].

[109] Informations disponibles sur le site de l'OFCOM: http://www.bakom.admin.ch [consulté le 08.05.2016].

[110] Informations disponibles sur le site internet de Skype: http://www.skype.com [consulté le 08.05.2016].

111 En deux ans de 2009 à 2013, le nombre d'abonnés VoIP est passé de 93 millions à plus de 300 millions[111], soit une tendance haussière de 322% en quatre ans.

b. La téléphonie au service de la justice

112 Avec l'évolution dans le secteur des télécommunications, la surveillance des correspondances – qui à l'origine englobait uniquement le courrier écrit – s'étend à la téléphonie. La surveillance téléphonique s'intègre alors dans un processus de protection de la sécurité publique[112].

113 En Suisse, sur 3'357 mesures de surveillances directes et 6'345 mesures de surveillance rétroactive[113] dont approximativement la moitié concerne la poursuite pour infractions graves à la loi sur les stupéfiants[114]. Par ailleurs, depuis 1998, la surveillance rétroactive a plus que doublé sur notre territoire.

114 Cet essor s'explique par la complexité de réseaux d'organisations criminelles, tels que les trafics de drogue, qui se développent considérablement depuis quelques années. Pour intercepter et court-circuiter les délinquants, les autorités pénales recourent à la surveillance des télécommunications. En effet, cette méthode d'échange est largement employée entre les divers trafiquants faisant parties de bandes organisées. Dès lors, la surveillance permet d'identifier les membres du réseau et de les confondre.

115 A noter qu'actuellement, les conversations VoIP sont épargnées par la surveillance des télécommunications, mais le répit est de courte durée un projet de modification du Code de procédure pénale étant en phase de consultation[115].

4. La vidéosurveillance

> "In general you could not assume that you were much safer in the country than in London. There were no telescreens, of course, but there was always

[111] IDATE, *DigiWorld Yearbook 2013*, Montpellier 2013, p. 80.

[112] BAERISWYL, Datenschutzrecht, p. 460; BONDALLAZ, protection des personnes, p. 522 ss; GEORGEL, p. 63.

[113] Infra Partie II, Chapitre 3, I, A, 1, b, n° 1109.

[114] Chiffres et informations disponibles sur le site internet du DFJP: http://www.ejpd.admin.ch [consulté le 08.05.2016].

[115] Infra Partie II, Chapitre 3, I, A, 4, c, I, n° 1328 ss.

the danger of concealed microphones by which your voice might be picked up and recognized [...]" (George Orwell)[116]

116 Soixante ans après la publication du livre "*1984*", l'imagination de George Orwell avec les télécrans – système de surveillance et de télévision qui diffusent en permanence les messages du Parti et surveillent simultanément les citoyens de Londres – devient réalité. Dans son livre, les télécrans sont l'égal des caméras de surveillance actuelles permettant à la "*police de la Pensée*" d'entendre et de voir ce qui se passe dans les lieux surveillés.

a. De la photo à la vidéo

117 De la simple photo, l'évolution des techniques mène à une série de photographies permettant de reconstituer un ensemble de mouvements, c'est la naissance du kinétographe ou kinétoscope. Puis, les pellicules de film se développant, les Frères Lumière font la première projection cinématographique le 28 septembre 1895[117].

118 De 1922 jusqu'en 1970, les perfectionnements se font sur les pellicules et la miniaturisation du matériel apportant deux innovations: l'enregistrement de l'image et du son, et la fabrication de la première caméra portative[118].

119 A partir de ces innovations, les recherches techniques vont s'axer exclusivement sur la qualité des images et sur leur traitement[119]. Enfin, les années 80 sont marquées par l'instauration des réseaux informatiques permettant le transport des images sur une courte distance. Puis, grâce à l'apparition de la fibre optique et l'utilisation des réseaux hertziens, la distance de la transmission vidéo n'est plus limitée.

120 L'arrivée du numérique a révolutionné la surveillance par caméras. Avec l'émergence de l'informatique et son intégration dans la vidéosurveillance, "*l'architecture récente*" comporte de nouvelles fonctionnalités utiles aux autorités: occultations électroniques, détections de mouvements ou d'agressions, transmissions par réseau téléphonique, enregistrements numérisés sur des disques durs, reconnaissances de caractères ou faciales, etc. Aujourd'hui, les progrès sont ciblés sur la qualité de l'image, les possibilités de zoom, la capacité des

---

[116] ORWELL George, *1984*, Londres 1949, p. 118.

[117] ENCYCLOPEDIE UNIVERSALIS, *Lumières (Philosophie des)*, 6ème éd., Paris 2008, Tome 14; PERES, p. 7.

[118] PERES, p. 9-12, 166 et 300; UEBERSCHLAG Josette, *Jean Brérault, l'instituteur cinéaste (1898-1973)*, Saint-Etienne 2007, p. 217.

[119] BAUER, FREYNET, p. 52-55.

disques durs pour l'enregistrement des vidéos et la vitesse de transmission des images capturées.

121 Relevons encore que ces dernières années, l'économie nippone est en effervescence avec la production d'appareils électroniques miniaturisés valant entre 345 CHF et 2305 CHF[120]. Ainsi, la surveillance est à portée de tous et plus spécifiquement des particuliers.

b. L'émergence de la vidéosurveillance

122 L'image a longtemps alimenté la preuve pénale. D'abord fixe sous forme de photographie, elle devient animée et, aujourd'hui, numérisée.

123 Suite à la reconnaissance de l'objectivité des images, les gouvernements se sont interrogés sur la nécessité d'installer des caméras de surveillance dans les lieux publics comme moyen sécuritaire et probatoire.

124 Depuis 1970, la vidéosurveillance dans sa fonction d'entraide à l'activité judiciaire et à la prévention des crimes est employée sur territoire anglais pour prévenir le terrorisme. Les résultats positifs de cette technologie sur ce territoire sont annoncés une dizaine d'années plus tard. L'utilité de la surveillance visuelle est alors reconnue. La France installe donc à son tour des systèmes de surveillance[121].

125 Poussée par un courant sociologique et politique, la vidéosurveillance se développe partout dans le monde durant les années 90 à 2000.

126 En réponse à l'augmentation de la délinquance, la Grande-Bretagne poursuit une politique de grande ampleur sur la vidéosurveillance. Aujourd'hui, le nombre exact de caméras sur le territoire anglais n'est pas connu, mais, dans un document de travail, Michael McCahill et Clive Norris estiment que ce nombre s'élève à 4,2 millions de caméras en Angleterre dont 500'000 dans la capitale[122]. Un londonien voit ainsi son image enregistrée en moyenne 300 fois par jour.

127 La Suisse ne déroge pas à la fonction sécuritaire de la vidéosurveillance principalement installée dans les parkings, les gares, les banques, les centres commerciaux ainsi que dans les transports publics. La Confédération ne dévoile aucun chiffre officiel. Pour estimer le

---

[120] BOUGON, TEMMAN, p. 22.

[121] BAUER, FREYNET, p. 3.

[122] MCCAHILL Michael, NORRIS Clive, CCTV in London, in *The Urbaneye working papers series* n° 6 (2002) p. 20.

nombre de caméras installées dans l'espace public suisse, Francisco Klauser se fonde sur le chiffre d'affaires des entreprises spécialisées dans le domaine de la surveillance par caméra. Il estime à environ 40'000 le nombre de caméras actives sur le territoire suisse en 2005, soit une caméra chaque kilomètre carré, dont 270 dans les rues de la ville de Genève[123].

128 Actuellement, sur terre, 25 millions de caméras sont recensées, mais – au vu des non-dits de certains gouvernements – ce chiffre peut ne pas refléter la réalité. Ces prochaines années et malgré les débats récents sur l'ingérence de la vidéosurveillance dans la vie privée, le nombre de caméras dans le monde devrait doubler, voire tripler.

5. Le Global Positioning System

a. La naissance du GPS et son utilisation

129 En 1957, l'impulsion nécessaire à la recherche et à la création du GPS est donnée. Suite au lancement du satellite russe *Spoutnik*, les scientifiques découvrent qu'à l'aide du signal radio émis par le satellite il est possible de suivre ses déplacements[124].

130 Une idée naît dans l'esprit des scientifiques et grandit: utiliser sur terre le système GPS pour déterminer la position d'un individu ou d'un lieu. Issu d'un projet de recherche de l'U.S Navy, le premier système GPS nommé TRANSIT est créé en 1960[125]. Treize ans plus tard, le système NAVSTAR – Navigation Satellite Timing And Ranging – déployé par le Pentagone prend le relais[126]. Ces dispositifs sont exclusivement réservés à l'usage militaire.

131 D'ailleurs, pour éviter l'utilisation des satellites par des civils, les quatre Bloc de satellite GPS des systèmes TRANSIT et NAVSTAR étaient munis de la fonction *Selective Availability*[127]. Ce système d'accès limitait la précision à une centaine de mètres pour tout utilisateur tiers de l'U.S Navy. Le 2 mai 2000, le Président américain Bill Clinton confirme l'intérêt du GPS à des fins civiles et demande la désactivation de la fonction *Selective Availability*[128]. La diffusion des signaux GPS n'étant plus restreinte, une précision inférieure à 20 mètres est possible sans correction de signal. En outre, les satellites de dernière génération – *Bloc IIR* – sont dotés de

---

[123] KLAUSER Francisco, A comparison of the impact of protective and preservative videosurveillance on urban territoriality: the case of Switzerland, in *Surveillance & Society* vol. 2 (2005) issue 2/3 p. 145-160.

[124] ANDRÉANI, p. 11; DODEL, HÄUPLER, p. 2.

[125] DODEL, HÄUPLER, p. 6; LEICK, p. 72.

[126] DODEL, HÄUPLER, p. 178-179; EL-RABBANY, p. 1.

[127] ANDRÉANI, p. 14; DILELLIO, GALVIN, RIZZO, p. 187; EL-RABBANY, p. 4; LEICK, p. 73.

[128] BARLIER, p. 82; DODEL, HÄUPLER, p. 196-197.

la fonction AUTONAV grâce à laquelle le satellite reste opérationnel lorsque le contact avec le récepteur GPS est rompu[129].

132 Actuellement, les systèmes de positionnement par satellites – opérationnels ou en cours de mise en place – sont au nombre de trois: le GPS (système américain d'origine militaire), le GLONASS (système soviétique repris partiellement par la Russie) et GALILEO (système européen). Ces systèmes s'appuient tous sur la triangulation tridimensionnelle afin de donner la position géographique des récepteurs[130].

133 Techniquement, les systèmes sont constitués d'une constellation de satellites qui gravitent autour de la terre sur plusieurs plans orbitaux – six pour le GPS et trois pour GALILEO – et émettent des signaux continus.

134 La localisation précise et la disponibilité des signaux vingt-quatre heures sur vingt-quatre indépendamment des conditions météorologiques ont pour conséquence la démocratisation de la technologie GPS dès le milieu de l'année 2000.

135 Les perfectionnements du système GPS ne sont actuellement qu'à leurs débuts. Les fonctions, la précision du signal et la durée de vie des satellites devraient subir des améliorations conséquentes permettant de faire perdurer le GPS au moins jusqu'en 2030.

b. L'utilisation du GPS comme moyen de surveillance

136 Aujourd'hui, le GPS connaît un succès considérable sur le plan civil, principalement dans le domaine de la navigation routière. En Suisse, environ 779'983 voitures de tourisme étaient équipées d'un GPS en 2007, ce qui veut dire qu'environ 20% des propriétaires de véhicules motorisés ont ou peuvent avoir recours à cette technologie[131]. Ce pourcentage ne cesse d'augmenter sans qu'une nouvelle statistique ne le démontre néanmoins[132].

---

[129] ANDRÉANI, p. 14; EL-RABBANY, p. 4; LEICK, p. 73.

[130] DODEL, HÄUPLER, p. 47; OOSTERLINK, p. 88-89.

[131] OFROU, *Les véhicules équipés d'un GPS*, Berne 2007, disponible sur: http://www.astra.admin.ch [consulté le 08.05.2016].

[132] OFROU, *Les véhicules équipés d'un GPS*, Berne 2013, disponible sur: http://www.astra.admin.ch [consulté le 08.05.2016].

137 Juridiquement, en Suisse, le GPS fait son apparition dans une jurisprudence rendue par le Tribunal fédéral le 21 mars 2005[133]. Cet arrêt relate l'utilisation de la localisation par GPS comme moyen de preuve.

138 En fait, la police a interpellé le prévenu et trouvé en sa possession le butin de onze vols commis dans des voitures. Le suspect avait une voiture munie d'un équipement GPS. Durant l'enquête, les policiers ont recueilli les données du GPS et les ont regroupées avec des scènes d'infractions similaires. Vingt-neuf autres commissions de vols ont ainsi pu être reprochées au prévenu.

139 Actuellement, l'exploitation d'informations provenant des GPS reste anecdotique par rapport à la localisation par téléphonie mobile. Le programme Via Sicura[134] et la diffusion toujours plus importante des équipements de géopositionnement conduira probablement – dans un futur proche – la police à exploiter régulièrement les données spatio-temporelles.

6. Les moyens informatiques

140 Le monde moderne emploie souvent le terme *ordinateur* comme synonyme du mot *informatique*. Il est erroné de restreindre l'informatique à des équipements électroniques de traitements automatiques de données. Originellement, l'informatique se définit comme la science du traitement rationnel. En d'autres termes, toutes les méthodes techniques facilitant le calcul ou le traitement d'informations s'intègrent à cette notion.

141 Contrairement à l'ordinateur né il y a à peine septante ans, l'informatique comprise dans son sens large date de plusieurs milliers d'années. L'homme a de tout temps créé des outils pour l'aider à calculer en limitant les erreurs et en économisant du temps.

a. Le développement de l'ordinateur

142 Quatre générations d'ordinateur se sont succédées depuis 1936[135]:

---

[133] ATF 1P.153/2005.

[134] Infra Partie II, Chapitre 3, II, B, 1, b, ii, n° 1697 ss; Infra Partie II, Chapitre 3, II, E, 1, c, iii, n° 1806 ss.

[135] BIRRIEN, p. 50, 53, 68 et 86-87; CERUZZI, p. 13-18, 51, 58, 64-70 et 218; FERRO, SWEDIN, p. 25-64 et 65-130; PAOLETTI, p. 45-46; PIGUET, HÜGLI, p. 72-90, 105-107 et 149-154; TURING Alan Mathison, On computable numbers with an application to the Entscheidungsproblem, in *Proceedings of London Mathematical Society* s2-42 (1937) p. 230-265.

- La première génération née en 1936 avec le Turing s'achève avec le premier IBM. De cette génération est issue la programmation informatique, la notion de programme informatique, les calculateurs électroniques et le traitement de nombres et de textes. En outre, dès 1939, les premiers systèmes de stockage font leur apparition avec de faibles capacités de 64 mots à leurs débuts jusqu'à 8'192 mots.
- De 1956 à 1973, les ordinateurs de deuxième génération sont une évolution des ordinateurs de première génération. Les innovations techniques se ciblent sur la miniaturisation, la robustesse, la légèreté des composants et la diminution de la consommation électrique. En outre, le RAMAC est créé. Il s'agit de l'ancêtre de notre disque dur qui permet de stocker 60'000 caractères. En revanche, le coût des ordinateurs et des systèmes de stockage est un frein à l'emploi de l'informatique.
- La troisième génération d'ordinateur (1963 à 1971) est marquée par la naissance de la puce électronique. Les composants informatiques continuent de se miniaturiser impliquant une diminution de la grandeur des ordinateurs et du coût de production, sans toutefois permettre l'accessibilité des ordinateurs au grand public.
- La quatrième génération est née en 1971. Tous les transistors se trouvent sur un seul circuit intégré, le coût de production devient alors faible et les ordinateurs deviennent peu à peu accessibles à tout un chacun. Quant à la mémoire de masse, les capacités de stockage des disques durs de troisième génération peuvent atteindre 25 milliards de caractères en 1998 et 1'000 milliards en 2007.

143 Malgré son jeune âge, le matériel informatique a subi une évolution colossale en passant d'un ordinateur de 50 tonnes nécessitant 25 kilowatts d'énergie et traitant une centaine d'instructions par seconde à un micro-processeur Pentium de quelques grammes consommant 25 watts et traitant 100 millions d'instructions à la seconde[136]. Entre 1980 et 2013, la vitesse de lecture et d'écriture des disques durs s'est multipliée par 32, leur durée de vie par 145. Parallèlement, leur coût d'achat a fortement chuté passant de 300 dollars le mégaoctet à 0,00022 dollars[137]. En trente-et-un ans, le prix du mégaoctet s'est divisé par 1,3 millions alors même que les disques durs se sont perfectionnés. En sus, la vitesse de calcul s'est améliorée et le coût d'un ordinateur a diminué. L'informatique devient un bien abordable pour tous.

144 Au début des années 50, une étude a estimé à une cinquantaine le nombre d'ordinateurs vendus. Aujourd'hui, plus d'un 1,5 milliards d'ordinateurs de quatrième génération sont en

[136] COHEN, VERDIER, BENGHOZI p. 169; FIGER, p. 1.

[137] Informations disponibles sur le site internet de Seagate: http://www.storageseagate.com [consulté le 09.10.2013].

fonction dans le monde entier[138]. En cinquante ans, le marché mondial a cru de 3 milliards de pourcents.

145 Si nous nous projetons en 2020, tout laisse à penser que le Pentium sera aussi démodé que la première génération d'ordinateurs et que les disques durs pourront stocker toujours plus d'informations à moindre coût.

146 Pour preuve de cette évolution, nous pouvons citer la *première loi de Moore*[139]. Constatant que la complexité des semi-conducteurs doublait toutes les années à coût constant depuis 1959, date de leur invention, Gordon Moore en déduit l'hypothèse suivante: la puissance va poursuivre cette croissance exponentielle. En 1975, Gordon Moore réévalue sa prédiction avec la *deuxième loi de Moore* et modifie le rythme de croissance. Désormais, le nombre de transistors des microprocesseurs sur une puce de silicium double tous les vingt-quatre mois, et non tous les douze mois. Bien qu'il ne s'agisse pas d'une loi physique, mais juste d'une extrapolation empirique, cette prédiction s'est révélée étonnamment exacte.

147 Théoriquement, la *deuxième loi de Moore* devrait cesser de s'appliquer en 2015, mais les barrières technologiques et les limites physiques empêchent cette progression. Actuellement, l'industrie informatique contourne cet obstacle par le doublement sur une même puce du nombre de processeurs, la fréquence restant, pour sa part, inchangée (Dual PowerPC en 2002, Dual IA en 2004, Intel Core Duo en 2006). Par ce biais, l'industrie informatique assure la continuité de l'évolution de la puissance des ordinateurs.

b. La création d'Internet

148 Avec la croissance du marché de l'informatique, l'idée d'un réseau informatique – permettant aux utilisateurs d'ordinateurs de communiquer entre eux – se développe.

149 De 1960 à 1980, les premiers réseaux dont l'ARPANET voient le jour permettant une communication générale entre des ordinateurs reliés par une ligne de télécommunication à large bande[140]. Relevons que l'ARPANET créé en 1969 est le précurseur d'Internet[141].

---

[138] Chiffre disponible sur le site internet de Computer Industry Almana Inc: http://www.c-i-a.com/ [consulté le 08.05.2016].

[139] MOORE Gordon, Cramming more components onto integrated circuits, in *Electronics magazine* vol. 38 (19 avril 1965), disponible sur: http://download.intel.com/research/silicon/moorespaper.pdf [consulté le 08.05.2016].

[140] CERUZZI, p. 259; LICKLIDER Joseph Carl Robnett, Man-computer symbiosis, in *Human factors in electronics* HFE-1 (1960) p. 4-11.

[141] BIRRIEN, p. 90; CERUZZI, p. 117.

Initialement financé à des fins militaires, ce réseau va se déployer uniquement au sein des universités américaines.

150 Avec le développement d'ARPANET, divers protocoles réseaux se créent amenant un besoin d'uniformisation, c'est ainsi que naît le protocole TCP/IP – Transmission control Protocol/Internet Protocol – intégré officiellement dans l'ARPANET en 1983[142].

151 La fusion d'ARPANET avec le NFSNet créé par la "*National Science Fondation*" pose la dernière pierre nécessaire à la création de l'Internet moderne se définissant comme le réseau mondial rassemblant l'ensemble des réseaux d'ordinateurs et utilisant le protocole TCP/IP pour communiquer[143].

152 Au début des années 1980, Tim Berners-Lee, chercheur au CERN, s'intéresse à la problématique des moyens de recherche et d'organisation de l'information. Il met au point un système de navigation hypertexte[144]. A la fin des années 1990, il instaure le protocole HTTP – Hyper Text Transfer Protocol – ainsi que le langage HTML[145] – Hypertext Markup Language – permettant de naviguer à l'aide de liens hypertextes à travers tous les réseaux.

153 L'application de Tim Berners-Lee donne naissance au *World Wide Web* qui se diffuse rapidement. En 1996, plus de 30 millions de pages publiques d'informations étaient référencées dans les systèmes de recherche[146].

154 L'influence de l'informatique sur la société est aujourd'hui officiellement reconnue. Avant l'unification du protocole réseau – TCP/IP – et la création du *World Wide Web*, seulement 1'000 ordinateurs étaient connectés au réseau. Vingt-cinq ans plus tard, 1,733 milliards de personnes sont raccordées à Internet à travers le monde, et chaque seconde cinq nouveaux raccords sont effectués[147]. Selon les statistiques, Internet a encore un bel avenir devant lui, son taux de pénétration actuel de 34,3% devant doubler d'ici 2017.

---

[142] COMER, p. 7; MURRAY, p. 69; O'REGAN, p. 105.

[143] CERUZZI, p. 295-296; COMER, p. 7-9; FIGER, p. 14.

[144] CERUZZI, p. 300-302; O'REGAN, p. 106-107.

[145] CERUZZI, p. 302; MURRAY, p. 4 et 72-74.

[146] FIGER, p. 15.

[147] Chiffres disponibles sur le site internet d'Internet world stats: http://www.internetworldstats.com [consulté le 08.05.2016].

c. L'Internet comme mode de communication

155 Le réseau ARPANET est une contribution majeure à l'essor des courriers électroniques[148]. En effet, lors de la création de ce réseau, des échanges expérimentaux de courriers inter-système ont été effectués[149]. Puis, en 1971, le programme SNDMSG/READMAIL – Send message/read message – est implanté dans ARPANET. En utilisant deux boîtes aux lettres électroniques sur deux ordinateurs situés côte-à-côte et connectés au réseau, Ray Tomlinson réussit à envoyer un message "QWERTYUIOP" et à le réceptionner. A cette occasion, l'ingénieur définit l'adresse électronique en reprenant le nom de l'utilisateur, le nom de l'ordinateur et en les séparant par un @[150].

156 Par la suite, l'amélioration des travaux de Ray Tomlinson permet de créer la première application capable de lister les messages par objet ou par date et de les lire dans l'ordre de son choix. Depuis l'instauration des messageries électroniques sur le réseau ARPANET, les programmes de courriels n'ont de cesse de croître.

157 Avec l'avènement du réseau informatique, les ingénieurs découvrent donc un moyen innovateur d'échange d'informations. Depuis, le courrier électronique est souvent considéré comme la *killer application* ou *application révolutionnaire* d'Internet.

158 Dorénavant, en moins d'une seconde, les utilisateurs d'Internet et des messageries électroniques s'échangent, presque gratuitement, des données et des informations à travers le monde. C'est pourquoi, après la consultation des sites Web, l'email se classe en deuxième position des services les plus utilisés sur le net. En 1996, le service de courriers électroniques gratuit *Hotmail* de la société Microsoft recensait 100'000 utilisateurs et le chiffre s'élevait à 30 millions d'abonnés fin 1998[151]. Environ dix ans plus tard, le nombre de comptes email dépasse les 3,9 milliards, près de 200 millions de nouveaux comptes sont créés chaque année[152].

159 Simple, rapide et gratuite, la globalisation des messageries électroniques se reflète dans l'augmentation sensible du volume des communications écrites. En ne comprenant pas les spams, ce n'est pas moins de 183 milliards d'emails qui sont envoyés chaque jour, dont

---

[148] CERUZZI, p. 298; LICKLIDER Joseph Carl Robnett, Applications of information networks, in *Computer-supported cooperative work: a book of readings* vol. 66 n° 11, p. 143-183.

[149] CERUZZI, p. 259; WAGNER, HÜTTL, BAKIN, p. 65; SAFKO, p. 62.

[150] RAHOUAL, SIARRY, p. 15; WAGNER, HÜTTL, BAKIN, p. 65-66; WATSON, p. 175.

[151] Informations fournies par la société Hotmail.

[152] Informations disponibles sur le site internet The Radicati Group Inc: http://www.radicati.com/ [consulté le 08.05.2016].

environ 82 milliards de personne à personne, ce qui ne comprend pas les emails professionnels[153]. Avec 3.9 milliards de comptes emails, chaque abonné envoie près deux messages électroniques toutes les heures.

d. Les technologies de l'information au service de la police et de la justice

160 Les technologies informatiques comme l'ordinateur, l'Internet et le courrier électronique se sont largement diffusés et sont devenus des commodités quasiment nécessaires, ce qui n'a pas échappé aux institutions policières et judiciaires.

161 En outre, accompagnant l'émergence de l'informatique et l'Internet, de nouvelles criminalités ont vu le jour telles que le trafic d'images pornographiques enfantines *via* le Peer-to-Peer ou au travers de groupes fermés. Pour lutter contre ces nouvelles criminalités, la police recours aux technologies informatiques, notamment en surveillant les adresses IP[154].

162 Historiquement, le combat contre la criminalité informatique est récent, mais aucune date précise n'est fournie quant au premier traçage IP effectué. En Suisse, l'opération *Genesis* de 2002 menée pour lutter contre les sites internet relevant de la pornographie enfantine est la première opération d'ampleur nationale[155]. Six mois après le début de l'opération *Genesis*, le service de coordination de la lutte contre la criminalité sur Internet – SCOCI – voit le jour[156]. Dorénavant, en sus des brigades de criminalité informatique cantonales – autorisées par la loi[157] –, le service fédéral recherche quotidiennement le contenu illicite sur Internet et identifie les suspects à l'aide de l'adresse IP.

163 Les criminels ont également vite cerné l'avantage des communications par messageries électroniques. Connaissant la possibilité d'écoutes téléphoniques, les conversations écoutées deviennent de moins en moins intéressantes. Les délinquants utilisant fréquemment les emails pour communiquer, il est devenu rapidement nécessaire de surveiller ce mode de communication.

---

[153] Informations disponibles sur le site internet d'IDC – Analyze the future: http://www.idc.com/ [consulté le 08.05.2016].

[154] Informations disponibles sur le site internet du SCOCI: http://www.kobik.ch [consulté le 08.05.2016].

[155] Proposition du groupe de travail, p. 1.

[156] Proposition du groupe de travail, p. 4.

[157] Infra Partie II, Chapitre 3, III, A, 5, a, i, n° 2118 ss; Infra Partie II, Chapitre 3, IV, B, n° 2205.

164 Ainsi, pour lutter contre la criminalité, prouver un fait ou identifier les auteurs d'une infraction, les autorités policières et judiciaires ont su tirer les avantages des technologies informatiques.

CHAPITRE 2: LE SIÈGE DE LA MATIÈRE

165 Le droit de la preuve trouve ses fondements à presque tous les niveaux de l'ordre juridique suisse. Afin de poser les bases juridiques de ce droit, spécifiquement des moyens de preuves scientifiques ou techniques, nous passons en revue le droit international (I.), le droit fédéral (II. A.) et, succinctement, le droit cantonal (II. B.) pertinents en mentionnant l'importance de ces actes, leurs droits et/ou garanties consacrés concernant la preuve pénale et leurs champs d'application.

I. Le droit international

166 Les garanties des droits fondamentaux et les principes généraux de procédure proviennent des règles internationales pouvant être assemblées en deux catégories: les instruments universels de protection des droits de l'homme (A.) et les instruments régionaux de protection des droits de l'homme (B.)

A. Les instruments universels de protection des droits de l'homme

1. La Déclaration universelle des droits de l'homme – DUDH

a. Sa place dans l'ordre juridique

167 Pour combattre les violations des règles élémentaires de la civilisation par les trois principales nations de l'Axe – l'Allemagne nazie, l'Italie fasciste et l'Empire du Japon –, les Alliés ont sollicité le rétablissement d'un ordre dans lequel les peuples et les individus vivront libres, en paix et jouiront des droits inhérents à leur qualité sans ingérence[158]. Pour ce faire, ils proposent une nouvelle organisation internationale – les Nations Unies – qui adopte en 1945 une Charte définissant les buts et principes de l'organisation et réaffirme la "*foi dans les droits fondamentaux de l'homme, dans la dignité et la valeur de la personne humaine*"[159].

[158] EMMERSON, ASHWORTH, MACDONALD, p. 2; ROBINSON, p. xix.

[159] Préambule de la Charte des Nations Unies du 26 juin 1945, RS 0.120.

168 Pour mettre en œuvre cette Charte, les organes des Nations Unies adoptent notamment la Déclaration universelle des droits de l'homme (DUDH) qui est approuvée à l'unanimité le 10 décembre 1948 par l'Assemblée générale des Nations Unies[160].

169 La DUDH est le premier instrument universel reconnaissant les droits de l'homme[161]. Bien que dépourvue de force contraignante pour les Etats, la DUDH n'en reste pas moins un outil précieux qui est à l'origine de divers accords internationaux – notamment de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et du Pacte international sur les droits civils et politiques – et de diverses lois nationales consacrées à la protection des droits humains[162].

b. Les droits devant idéalement être garantis

i. La DUDH et le droit de la preuve

170 L'article 11 DUDH prévoit les principes minimaux à respecter lorsqu'une personne est accusée d'un acte pénalement répréhensible[163]. L'article 11 § 1 DUDH énonce deux garanties fondamentales de procédure: la présomption d'innocence (11 § 1 *in limine* DUDH) et les droits de la défense (11 § 1 *in fine* DUDH).

171 L'article 11 § 1 in limine DUDH mentionne que "[t]oute personne accusée d'un acte délictueux est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie [...]". La notion d'une culpabilité "établie" fait référence à la vérité matérielle obtenue, notamment, grâce aux moyens de preuves. Ainsi, la présomption d'innocence implique deux règles, l'une sur l'administration des preuves, l'autre sur le fardeau de la preuve[164]. Par ailleurs, la présomption d'innocence s'accompagne du droit pour l'accusé de se taire ou de ne fournir que des preuves à décharge[165].

---

[160] United Nations Resolution 217 A (III) proclaiming a Universal Declaration of Human Rights, Paris 10 décembre 1948, A/RES/3/217 A, disponible sur: http://www.un.org [consulté le 08.05.2016].

[161] DSG-EPINEY, SCHLEISS, p. 58; KÄLIN, EPINEY, CARONI, KÜNZLI, p. 277-278; ROBINSON, p. 33; VERNIORY, p. 20.

[162] Message, ONU, p. 676; EMMERSON, ASHWORTH, MACDONALD, p. 2.

[163] ROBINSON, p. 115; VERNIORY, p. 21.

[164] AUER, MALINVERNI, HOTTELIER, vol. II, p. 621; JOSEPH, SCHULTZ, CASTAN, p. 426; MÜLLER, SCHEFER, p. 981-984; TRECHSEL, Human Rights, p. 167. Infra Partie I, Chapitre 3, III, A, n° 285 ss.

[165] Infra Partie I, Chapitre 2, I, A, 2, b, ii, n° 188.

172 Les droits de la défense, cités à l'art. 11 § 1 *in fine* DUDH, renferment le droit offert à l'accusé d'être entendu et le droit d'accès au dossier[166]. Résultante du principe de contradiction des débats, ces deux droits impliquent le droit de produire des preuves et le droit de participer à l'administration des preuves essentielles ou du moins de pouvoir s'exprimer sur le sujet[167].

ii. Quelques garanties essentielles en procédure pénale

173 La DUDH édicte également certaines garanties générales relatives aux droits de l'homme comme la dignité humaine et le respect de la sphère privée.

174 La dignité humaine est un droit inné de tout être humain[168]. Il s'entend principalement négativement comme le droit de ne pas être offensé ou blessé dans sa qualité humaine[169]. Suite à l'adoption de la DUDH, une multitude de textes internationaux sont venus compléter les droits fondamentaux prévus dans cette Déclaration. Tous – sans exception – reposent sur le concept de la dignité humaine tel qu'il est proclamé dans le préambule de la DUDH ainsi qu'à son article premier.

175 Concernant le respect de la sphère privée, l'art. 12 DUDH consacre des obligations négatives pour les Etats[170]. Ainsi, ils ne doivent pas violer arbitrairement la vie privée des individus en protégeant la vie familiale, le domicile et la correspondance des citoyens. La DUDH n'ayant pas force juridique, la jurisprudence n'a pas développé la notion de "*vie privée*" au sens de cette Déclaration. Le Pacte II[171], la CEDH et lois fédérales reposant en partie sur la DUDH, les interprétations et définitions faites des termes "*vie privée*" sont applicables par analogie[172].

---

[166] RIEDO, FIOLKA, NIGGLI, p. 9; ROBINSON, p. 115; VERNIORY, p. 20.

[167] ROBINSON, p. 115; VERNIORY, p. 20.

[168] MORSINK, p. 290; MÜLLER, SCHEFER, p. 1.

[169] BELSER, WALDMANN, MOLINARI, p. 7; HÄFELIN, HALLER, KELLER, p. 111; MÜLLER, SCHEFER, p. 1-2; ROBINSON, p. 103-104.

[170] MORSINK, p. 134; ROBINSON, p. 117.

[171] Pacte international du 16 décembre 1966 relatif aux droits civils et politiques (Pacte II), RS 0.103.2.

[172] Infra Partie I, Chapitre 2, I, A, 2, b, i, n° 183; Infra Partie I, Chapitre 2, I, B, 1, b, ii, n° 199; Infra Partie I, Chapitre 2, II, A, n° 217, 219-220.

c. Son champ d'application

176 En proclamant la DUDH, l'Assemblée générale des Nations Unies tente d'imposer aux Etats et à leur population un idéal à atteindre convenant à tous: hommes, femmes, enfants et pouvoir étatique[173].

177 Le préambule de la DUDH prévoit un champ d'application personnel large en plaçant sur pied d'égalité – sans distinction quant à la race, au sexe, à la religion, etc. – tous les êtres humains demeurant dans les Etats parties. Ces Etats sont chargés de protéger et de garantir les droits proclamés à leur population, y compris aux habitants des territoires placés sous leur juridiction.

178 Concernant le champ d'application matériel relatif au droit de la preuve, l'art. 11 § 1 DUDH est une prérogative nécessaire au respect de la présomption d'innocence qui fonde éthiquement le droit actuel.

2. Le Pacte international relatif aux droits civils et politiques – Pacte II

a. Sa place dans l'ordre juridique

179 Le Pacte international relatif aux droits civils et politiques – Pacte II – est conclu à New York le 16 décembre 1966[174]. Reconnaissant la dignité humaine et l'égalité des êtres humains comme fondement de la liberté, de la justice et de la paix et ayant une force contraignante pour les Etats parties, le Pacte II concrétise sur le plan international la Charte des Nations Unies et la DUDH.

180 En Suisse, le Pacte II est approuvé par l'Assemblée fédérale le 13 décembre 1991, ratifié par le Conseil fédéral le 18 juin 1992 et entré en vigueur le 18 septembre 1992.

181 En tant que traité multilatéral, le Pacte II est au sommet de la hiérarchie des normes. En vertu de l'art. 190 Cst[175]: "*Le Tribunal fédéral et les autres autorités sont tenus d'appliquer les*

---

[173] MORSINK, p. 12; ROBINSON, p. 36.

[174] Resolutions adopted by the General Assembly 2200 (XXI): International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, New York 16 décembre 1966, A/RES/21/2200, disponible sur: http://www.un.org [consulté le 08.05.2016].

[175] Constitution fédérale de la Confédération suisse (Cst) du 18 avril 1999, RS 101.

lois fédérales et le droit international". Ainsi, selon la conception moniste de la Suisse[176], le droit international s'impose aux juges nationaux qui doivent rendre leur décision conformément aux principes universels.

b. Les droits garantis

i. Les similitudes entre le Pacte II et la DUDH

182 Les articles sur la dignité humaine (Préambule et art. 10 § 1 Pacte II), la présomption d'innocence (art. 14 § 2 Pacte II) et la protection de la sphère privée (art. 17 § 1 Pacte II) sont repris – quasiment mot pour mot – du préambule et des articles de la Déclaration. L'analyse de ces principes sous l'angle du Pacte II est par conséquent similaire à celle de la DUDH.

183 Toutefois, une précision doit être apportée quant à la notion de "*sphère ou vie privée*". La doctrine définit la "*vie privée*" comme un choix, une fonction, un désir, un droit et/ou un besoin de l'individu d'avoir une sphère intime, voire secrète[177]. Elle s'assimile au droit de contrôler les informations que l'on désire dévoiler sur soi. Ainsi, la protection de l'art. 17 § 1 Pacte II protège les individus contre les intrusions injustifiées et abusives dans le domaine de l'autonomie individuelle[178].

ii. Le Pacte II et les garanties procédurales

184 Les garanties procédurales édictées à l'art. 14 Pacte II complètent et renforcent les concepts minimaux introduits par la DUDH.

185 L'art. 14 § 1 fait référence à l'équité des débats ainsi qu'à l'indépendance et à l'impartialité du tribunal décideur.

186 L'équité des débats est une notion qui doit se lire en relation avec les trois paragraphes de l'art. 14 Pacte II qui élaborent des garanties minimales non-exhaustives: indépendance et impartialité des tribunaux, présomption d'innocence, droit d'être entendu, droit de disposer

---

[176] AUER, HOTTELIER, MALINVERNI, Vol. I, p. 455; DSG-EPINEY, SCHLEISS, p. 53; WIEDERKEHR, RICHLI, p. 372.

[177] JOSEPH, SCHULTZ, CASTAN, p. 476; MAHON, p. 124-125; MEYER-LADEWIG, art. 8 N 78; RHINOW, SCHEFER, p. 260-261.

[178] OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *Observation générale no 16: Le droit au respect de la vie privée, de la famille, du domicile, et le droit d'être protégé contre les atteintes à l'honneur et à la réputation (art. 17)*, Genève 1988, disponible sur: http://www.unhchr.ch [consulté le 08.05.2016].

du temps et des facilités nécessaires à sa défense, etc.[179]. Ces garanties peuvent ne pas suffire, raison pour laquelle la Cour européenne délimite *in concreto* l'équité des débats[180].

187 L'indépendance assurant la liberté d'esprit des juges et l'impartialité découlant de la loyauté des débats sont des exigences nécessaires à un procès équitable[181]. Relevons que l'impartialité s'apprécie subjectivement – déterminant la conviction et le comportement personnel d'un juge, cette impartialité est présumée – et objectivement – exclusion de tout doute légitime sur l'avis préliminaire d'un juge[182].

188 L'art. 14 § 3 Pacte II énumère non-exhaustivement toute une série de droits de la défense. Les lettres b – disposer des facilités nécessaire à sa défense –, e – droit d'interroger ou de faire interroger les témoins à charge ou à décharge – et g – droit au silence ou droit de ne pas s'auto-incriminer – se rapportent au droit de la preuve. Corollaire de l'égalité des armes et du principe de contradiction, selon le Comité des droits de l'homme, les "*facilités nécessaires*" de l'art. 14 § 3 let. b "*doivent comprendre l'accès aux documents et autres éléments de preuve dont l'accusé a besoin pour préparer sa défense* [...]"[183].

---

[179] Par analogie: CourEDH, Affaire *Adolf c. Autriche*, arrêt du 26 mars 1982, § 49; CourEDH Affaire *Goddi c. Italie*, arrêt du 9 avril 1984, 8966/80, § 28; CourEDH, Affaire *Poitrimol c. France*, arrêt du 23 novembre 1993, 14032/88, § 34; CourEDH, Affaire *Allenet c. France*, arrêt du 10 février 2005, 15175/89, § 35-36; CourEDH, Affaire *Dikme c. Turquie*, arrêt du 11 juillet 2000, 20869/92, § 108; CourEDH, Affaire *Luca c. Italie*, arrêt du 27 février 2001, 33354/96, § 21; CourEDH, Affaire *Brennan c. Royaume-Uni*, arrêt du 16 octobre 2001, 39846/98, § 45; CourEDH, Affaire *Demebukov c. Bulgarie*, arrêt du 28 février 2008, 68020/01, § 50; CourEDH, Affaire *Salduz c. Turquie*, arrêt du 27 novembre 2008, 36391/02, § 50-55; OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *Observation générale no 13 L'égalité devant les tribunaux et le droit d'être entendu équitablement et publiquement par un tribunal indépendant et établi par la loi (art. 14)*, Genève 1984, disponible sur: http://www.unhchr.ch [consulté le 08.05.2016], § 5.

[180] CourEDH, Affaire *Adolf c. Autriche*, arrêt du 26 mars 1982, § 49; CourEDH Affaire *Goddi c. Italie*, arrêt du *9 avril 1984*, 8966/80, § 36-41; CourEDH, Affaire *Colozza c. Italie*, arrêt du 12 février 1985, 9024/80, § 27; CourEDH, Affaire *Feldbrugge c. Pays-Bas*, arrêt du 29 mai 1986, 8562/79, § 44; CourEDH, Affaire *Barberà, Messegué et Jabardo c. Espagne*, arrêt du 6 décembre 1988, 10590/83, § 83; CourEDH, Affaire *Murray c. Royaume-Uni*, arrêt du 8 février 1996, 18731/91, § 45; CourEDH, Affaire *Werner c. Autriche*, arrêt du 24 novembre 1997, 21835/93, § 45; CourEDH, Affaire *Pisano c. Italie*, arrêt du 27 juillet 2000, 36732/97, § 21; CourEDH, Affaire *Salduz c. Turquie*, arrêt du 27 novembre 2008, 36391/02, § 50-55.

[181] HÄFELIN, HALLER, KELLER, p. 266-267; JEANNERET, KÜHN, p. 41; MEUNIER, p. 192; MÜLLER, SCHEFER, p. 821, 948 et 955-956.

[182] GRABENWARTER, PABEL, p. 407-413; HARRIS, O'BOYLE, WARBRICK, p. 284; HOTTELIER, MOCK, PUÉCHAVY, p. 147-148; JEANNERET, KÜHN, p. 42-43; MEYER, art. 6 N 43; MEYER-LADEWIG, art. 6 N 68-71 et 70-79. Infra Partie I, Chapitre 3, III, C, n° 313 ss.

[183] OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *Observation générale n° 13: L'égalité devant les tribunaux et le droit d'être entendu équitablement et publiquement par un tribunal indépendant et établi par la loi (art. 14)*, Genève 1984, disponible sur: http://www.unhchr.ch [consulté le 08.05.2016], § 9.

189 Spécifions que le Pacte II est le seul texte à formuler explicitement le droit de ne pas s'exprimer au cours de son procès découlant de l'adage "*nemo tenetur seipsum prodere vel accusare*". Savoir si le droit de se taire est assimilable au droit de ne pas s'incriminer soi-même est controversé en doctrine dont une partie considère que le droit de se taire va moins loin que le droit de s'abstenir de collaborer activement[184]. En droit suisse, cette controverse a peu d'importance dès lors que la charge de la preuve revient à l'accusation. L'accusé est donc en droit de n'apporter aucun élément probatoire.

c. Son champ d'application

190 L'article 2 § 1 Pacte II prévoit le principe d'égalité entre les hommes indifféremment de toutes distinctions. En procédure pénale, la dérogation à ce principe est formellement exclue (art. 14 § 1 Pacte II)[185]. Par ailleurs, le champ d'application personnel est restreint à l'art. 14 Pacte II puisque que les garanties qu'il institue ne servent qu'à protéger une personne accusée.

191 Quant au champ d'application matériel, le Pacte II prévoit une série de droits et de garanties inhérentes aux êtres humains. En revanche, aucune disposition n'est propre au droit de la preuve, mais l'art. 14 Pacte II reconnaît de manière implicite la nécessité d'administrer des preuves[186].

[184] CourEDH, Affaire *Saunders c. Royaume-Uni*, arrêt du 17 décembre 1996, § 68-69; CourEDH, Affaire *J.B. c. Suisse*, arrêt du 3 mai 2001, 31827/96, §64; CourEDH, Affaire *Jalloh c. Allemagne*, arrêt du 11 juillet 2006, 54810/00, § 100; CourEDH, Affaire *Kolu c. Turquie*, arrêt du 2 août 2005, 35811/97, § 51; CourEDH, Affaire *O'Halloran et Francis c. Royaume-Uni*, arrêt du 29 juin 2007, 15809/02 et 25624/02, § 53-63; CourEDH, Affaire *Brusco c. France*, arrêt du 14 octobre 2010, 1466/07, § 44; EICKER, HUBER, p. 115; HÄNER, p. 23; HARRIS, O'BOYLE, WARBRICK, p. 259-260; MEYER-LADEWIG, art. 16 N 131; PETTITI, p. 141; TRECHSEL, Human Rights, p. 166; VERNIORY, p. 406.

[185] JOSEPH, SCHULTZ, CASTAN, p. 408-409; MÜLLER, SCHEFER, p. 879; VERNIORY, p. 25.

[186] CourEDH, Affaire *Daktaras c. Lituanie*, arrêt du 10 octobre 2000, 42095/98, § 41; CourEDH, Affaire *Huseyn et autre c. Azerbaijan*, arrêt du 26 juillet 2011, 35485/05, 35680/05, 36085/05, 45553/05, § 225; CourEDH, Affaire *Viravyan c. Arménie*, arrêt du 2 octobre 2012, 40094/05, § 185.

B. Les instruments régionaux de protection des droits de l'homme

1. La Convention européenne des droits de l'homme – CEDH

a. Sa place dans l'ordre juridique

192 Au niveau universel, les Pactes des Nations Unies prirent du temps – trente années se sont écoulées entre la mise en vigueur de la Charte des droits de l'homme et ses compléments, Pactes I et II – à être élaborés. Face à cette paralysie, la nécessité de mettre en place un système régional de protection apparaît dans l'esprit des gouvernements européens. La Convention de sauvegarde des droits de l'homme et des libertés fondamentales – usuellement appelée la Convention européenne des droits de l'homme et abrégée CEDH – est conclue le 4 novembre 1950 à Rome[187]. En sa qualité de traité multilatéral, elle est contraignante pour les Etats parties.

193 En Suisse, la CEDH entre en vigueur le 28 novembre 1974 avec la ratification du texte par le Conseil fédéral. En tant que traité, la CEDH est au sommet de la hiérarchie des normes[188].

194 Les articles 2 à 18 de la CEDH étant directement applicables – "*self-executing*"[189] –, ils confèrent aux particuliers, sans mesure d'exécution interne, des droits et des obligations pouvant – en cas de violation – être portés devant les instances judiciaires, comme le prévoit la Constitution fédérale à son art. 189 al. 1 let. b[190].

195 Relevons encore que la Constitution fédérale suisse reprend les garanties fondamentales établies par la CEDH[191]. A ce sujet, la doctrine et la jurisprudence relèvent qu'en vertu de l'art. 53 CEDH, les particuliers peuvent se prévaloir des garanties qui leur confèrent la meilleure protection. Le Tribunal fédéral peine à appliquer la CEDH en déclarant que les droits garantis par la Convention ne sont pas plus étendus que les normes constitutionnelles, dès lors que les juges interprètent abstraitement les articles constitutionnels en y incluant les apports conventionnels. Néanmoins, la pratique des tribunaux fédéraux tend à rééquilibrer la

---

[187] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 42; CEDH-DÉCAUX, p. 4; GRABENWARTER, PABEL, p. 2; HARRIS, O'BOYLE, WARBRICK, p. 1.

[188] HOTTELIER, MOCK, PUÉCHAVY, p. 13; VERNIORY, p. 34; VILLIGER, p. 649-650.

[189] GRISEL E, p. 3; HAEFGLIGER, SCHÜRMANN, p. 37; HÄFELIN, HALLER, KELLER, p. 76

[190] EMMERSON, ASHWORTH, MACDONALD, p. 32 et 92-93.

[191] BELSER, WALDMANN, MOLINARI, p. 9-10; HÄFELIN, HALLER, KELLER, p. 73; VILLIGER, p. 653.

balance en admettant que le champ d'application des normes conventionnelles est plus large que les garanties constitutionnelles[192].

b. Les droits garantis

i. Les similitudes entre la CEDH, le Pacte II et la DUDH

196 A la lecture des dispositions de la CEDH, de fortes similitudes avec le Pacte II sont décelables tant du point de vue des droits institués que de leur champ d'application matériel. Un simple renvoi aux explications des droits garantis par la DUDH et le Pacte II peut être fait concernant: le procès équitable (art. 6 § 1 CEDH à lire en relation avec le § 2 et 3), l'indépendance et l'impartialité des tribunaux concrétisant la maxime *in dubio pro reo* (art. 6 § 1 et 2 CEDH), le droit de disposer des facilités nécessaires à la préparation de sa défense (art. 6 § 3 let. b CEDH), et le droit d'interroger ou de faire interroger les témoins (art. 6 § 3 let. d CEDH)[193]. Le principe de la présomption d'innocence (art. 6 § 2 CEDH), le respect de la vie privée et familiale (art. 8 CEDH)[194], ainsi que le respect de la dignité humaine demandent quelques précisions.

197 A la lecture de l'art. 6 CEDH et contrairement à l'art. 14 § 3 let. g Pacte II, la Convention n'explicite pas le droit au silence, ni celui de ne pas contribuer à sa propre incrimination. Néanmoins, la Cour de Strasbourg a conclu que ces droits constituent une composante essentielle de la présomption d'innocence[195].

198 Quant à la dignité humaine, la CEDH ne contient pas de références explicites à ce sujet. Néanmoins, la philosophie qu'encourage la Convention est cohérente avec la défense de la dignité humaine à l'instar des autres instruments internationaux relatifs aux droits de l'homme. Les décisions de la Cour de Strasbourg confirment l'objectif général du respect de la dignité humaine. Dans l'affaire *Pretty c. Royaume-Uni*[196], la plus significative en la matière, la Cour a conclu que "*[l]a dignité et la liberté de l'homme sont l'essence même de la Convention.*";

---

[192] ATF 129 I 151, 153-154 = JdT 2005 IV 186, 187-188; ATF 131 I 476, 479-480.

[193] RIEDO, FIOLKA, NIGGLI, p. 9.

[194] CourEDH, Affaire *Botta c. Italie*, arrêt du 24 février 1998, 21439/93, § 32; CourEDH, Affaire *Niemietz c. Allemagne*, arrêt du 16 décembre 1992, 13710/88, § 29; CourEDH, Affaire *von Hannover c. Allemagne*, arrêt du 24 juin 2004, 59320/00, § 50; CourEDH, Affaire *Avram et autres c. Modlavie*, arrêt du 5 juillet 2011, 41588/05, § 37.

[195] CourEDH, Affaire *Funke c. France*, arrêt du 25 février 1993, 10828/84, § 44; CourEDH, Affaire *Murray c. Royaume-Uni*, arrêt du 8 février 1996, 18731/91, § 45; CourEDH, Affaire *Saunders c. Royaume-Uni*, arrêt du 17 décembre 1996, 19187/91, § 68; CourEDH, Affaire *Gafgen c. Allemagne*, arrêt du 1er juin 2010, 22978/05, § 169 ss.

[196] CourEDH, Affaire *Pretty c. Royaume-Uni*, arrêt du 29 avril 2002, 2346/02, § 65.

cette décision est complétée par l'arrêt Gündüz c. Turquie[197], où nous pouvons lire que "*[…] la tolérance et le respect de l'égale dignité de tous les êtres humains constituent le fondement d'une société démocratique […]*". Bien que la dignité humaine soit littéralement inexistante dans la CEDH, son assise est indiscutée et indiscutable.

ii. La possibilité de restreindre la garantie de la sphère privée

199 Le champ d'application matériel du droit au respect de la vie privée et familiale n'est guère dissemblable entre les divers instruments internationaux (art. 8 CEDH, art. 17 § 1 Pacte II et art. 12 DUDH). En revanche, la CEDH prévoit la possibilité de restreindre la garantie de la sphère privée, ce dont ni la DUDH, ni le Pacte II dont l'amendement analogue a été refusé ne prévoient.

200 En lieu et place de la notion "*d'immixtions arbitraires"* contenue dans la DUDH et "*d'immixtions arbitraires ou illégales*" du Pacte II, l'art. 8 § 2 CEDH définit les contours des restrictions à la sphère privée. L'ingérence d'une autorité publique n'est acceptable que si une "*loi prévoit l'ingérence et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*" (art. 8 § 2 CEDH).

201 En outre, la Cour européenne a constaté une obligation positive pour les Etats en vertu de l'art. 8 CEDH. Ils doivent en effet protéger les individus contre les immixtions de la part de leurs semblables dans leur vie privée[198]. Il existe donc un effet appelé *réflexe indirect* dans cette norme conventionnelle[199].

c. Le champ d'application

202 A l'image de la DUDH et du Pacte II, la CEDH contient une clause de non-discrimination à l'art. 14 CEDH. La Convention a donc un champ d'application personnel étendu à toute personne humaine habitant sur le territoire d'un Etat membre.

---

[197] CourEDH, Affaire *Gündüz c. Turquie*, arrêt du 4 décembre 2003, 35071/97, § 40.

[198] CourEDH, Affaire *Airey c. Irlande*, arrêt du 09 octobre 1979, 6289/73, § 32; CourEDH, Affaire *X et Y c. Pays-Bas*, arrêt du 26 mars 1985, 8978/80, § 21; CourEDH, Affaire *K.U. c. Finlande*, arrêt du 2 décembre 2008, 2872/02, § 42.

[199] EMMERSON, ASHWORTH, MACDONALD, p. 191; HARRIS, O'BOYLE, WARBRICK, p. 362; LEGLER, p. 36; MEIER P., p. 80; MEYER, art. 6 N 143; MEYER-LADEWIG, art. 8 N 2.

203 En procédure pénale, les garanties protègent uniquement les accusés contre l'arbitraire répressif (art. 6 § 1 CEDH). Il faut rappeler ici que la notion d'"*accusation en matière pénale*" est une notion autonome établie par la Cour européenne, c'est-à-dire qu'elle ne tient pas lieu des définitions nationales[200]. En termes brefs, la "*matière pénale*" englobe les faits ou les comportements liés à une infraction de droit national ou de nature pénale. Le but et la sévérité de la sanction fournissent également un indicateur quant à la nature de l'affaire. L'"*accusation*" se définit promptement comme l'acte de l'autorité compétente reprochant à un individu d'avoir commis une infraction.

204 Quant au champ d'application matériel, il comprend de nombreux droits et garanties, notamment dans le domaine de l'administration des preuves (art. 6 § 1 à 3 CEDH)[201].

2. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – Convention STE n° 108[202]

a. Sa portée juridique

205 Sous l'égide du Conseil de l'Europe, la Convention STE n°108 est conclue le 28 janvier 1981. Le Conseil fédéral ratifie cet instrument en date du 2 octobre 1997, qui entre en vigueur le 1er février 1998. La Convention STE n° 108 complémente et concrétise les articles 8 à 10 CEDH dans le domaine du traitement automatisé des données à caractère personnel afin de protéger les individus face au risque du traitement de données et d'harmoniser les législations nationales sur le plan européen en instaurant un standard minimum[203].

206 Contrairement aux instruments internationaux, la Convention STE n° 108 consacre des dispositions-programmes qui ne sont donc pas directement applicables, comme le prévoit

---

[200] CEDH-SOYER, SALVIA, p. 254-256; GRABENWARTER, PABEL, p. 392-393; HARRIS, O'BOYLE, WARBRICK, p. 205.

[201] CourEDH, Affaire *Adolf c. Autriche*, arrêt du 26 mars 1982, 8269/78, § 49; CourEDH Affaire *Goddi c. Italie*, arrêt du *9 avril 1984*, 8966/80, § 28; CourEDH, Affaire *Lutz c. République fédérale d'Allemagne*, arrêt du 25 août 1987, 9912/82, § 52; CourEDH, Affaire *Dikme c. Turquie*, arrêt du 11 juillet 2000, 20869/92, § 108; CourEDH, Affaire *Luca c. Italie*, 33354/96, arrêt du 27 février 2001, § 21.

[202] Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE n° 108), RS 0.235.1.

[203] EPINEY, HOFSTÖTTER, MEIER, THEUERKAUF, p. 50; MEIER P., p. 85; Message, Convention à l'égard du traitement automatisé, p. 704-705; STÄMPFLI, p. 111.

l'art. 4 al. 1: "*Chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncées […]*"[204].

207 En adoptant la LPD[205], la Suisse a comblé les lacunes existantes en matière de protection des données à caractère personnel. Cette loi garantit un niveau de protection adéquat au niveau fédéral. Les cantons disposent également d'une protection adéquate. Au moment de la mise en vigueur de cet instrument international, seize cantons[206] étaient dotés d'une législation sur la protection des données; un canton[207] intégrait des dispositions minimales dans son Code de procédure administrative; six cantons[208] avaient une disposition de protection des données personnelles dans leur Constitution; quatre cantons[209] avaient édicté des directives et respectaient l'art. 37 LPD lors du traitement de données en lien avec le droit fédéral; cinq[210] ne disposaient d'aucune base légale précise, mais ils étaient soumis à la LPD.

b. Les droits garantis

208 L'objectif de la Convention STE n° 108 est de permettre d'assurer un niveau élevé de protection aux personnes sujettes aux traitements automatisés, tout en ne paralysant pas la libre circulation transfrontalière des informations[211].

209 A cette fin, les données à caractère personnel doivent tout d'abord revêtir une certaine qualité pour être traitées (art. 5 Convention STE n° 108) et les données dites sensibles demandent une garantie normative appropriée (art. 6 Convention STE n° 108). En outre, toutes les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être sécurisées tant du point de vue technique qu'organisationnel (art. 7 Convention STE n° 108). Enfin, l'art. 8 Convention STE n°108 édicte une garantie formelle – découlant des libertés personnelles et du droit à l'autodétermination informationnelle – permettant aux individus concernés par de tels traitements informatisés de faire valoir leurs droits.

---

[204] BONDALLAZ, protection des personnes, p. 91 et 104; DSG-EPINEY, SCHLEISS, p. 79-80; Message, Convention à l'égard du traitement automatisé, p. 705.

[205] Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1.

[206] BL, BS, BE, FR, GE, JU, LU, NE, SH, SW, TI, TG, VS, VD, UR et ZH.

[207] SG.

[208] AG, BL, BE, GL, JU et SO.

[209] AG, AR, GR et SO.

[210] AI, GL, NW, OW et ZG.

[211] DSG-EPINEY, SCHLEISS, p. 84; MEIER P., p. 86; Message, Convention à l'égard du traitement automatisé, p. 705 et 714.

210 Dans le strict respect des conditions prévues à l'art. 9 Convention STE n° 108, les ingérences sont possibles moyennant une réglementation dans une loi nationale, la justification d'un intérêt public prépondérant, le respect du principe de proportionnalité mais également que le noyau intangible ne soit en aucun cas touché.

c. Le champ d'application

211 A l'instar des instruments internationaux préalablement étudiés, la Convention STE n° 108 contient un champ d'application personnel étendu consacrant le principe de non-discrimination à toute personne physique résidant sur le territoire d'un Etat partie (art. 1er Convention STE n° 108).

212 Matériellement, le champ d'application est également large. Il couvre tous les fichiers et traitements automatisés de données personnelles du secteur privé et du secteur public. Toutefois, les Etats peuvent en vertu de l'art. 3 ch. 2 let. a de la Convention STE n° 108 déposer une liste de fichiers qui sont exclus du champ d'application de la Convention[212]. La Suisse a notamment exclu les fichiers nécessaires lors de procédures pénales pendantes, étant précisé que la protection découle directement du Code de procédure pénale[213].

213 Quant aux bases de données utilisées par la police, la Commission fédérale de la protection des données a reconnu que les enquêtes de police ne se déroulent pas obligatoirement dans le cadre d'une procédure pénale pendante. Ainsi, la Convention STE n° 108 et la LPD ne trouvent pas application lorsqu'un individu peut faire valoir ses droits en tant que partie (partie civile, prévenu ou ministère public). En revanche, lorsqu'avant une procédure pendante ou pour toute conservation après jugement entré en force – les autorités collectent, enregistrent et conservent des données d'un suspect ou de tiers, les droits et garanties imposés par la Convention STE n° 108 et la LPD doivent être respectés[214].

---

[212] Message, Convention à l'égard du traitement automatisé, p. 709-710.

[213] DSG-EPINEY, SCHLEISS, p. 84.

[214] A ce sujet, voir notamment: art. 99 al. 2 *cum* 103 CPP; art. 16 al. 1 Loi sur les profils d'ADN; art. 20 al. 2 let. a O-RIPOL.

II. Le droit interne

A. Le droit fédéral

1. La Constitution fédérale – Cst

a. Sa place dans l'ordre juridique

214 La Constitution fédérale de la Confédération suisse du 18 avril 1999 représente le sommet de la hiérarchie des normes internes. En réunissant, l'ensemble des règles juridiques importantes, elle est considérée à juste titre comme norme suprême[215].

215 La Constitution organise les tâches étatiques et légitime l'ordre juridique en limitant le pouvoir de l'Etat national, en déterminant les principes de base – notamment – des procédures judiciaires, en interdisant la violation de certaines garanties nécessaires à tout Etat de droit et en proscrivant l'arbitraire[216].

216 Par sa légitimation, la Constitution fédérale du 18 avril 1999 constitue une source primordiale et impérative en droit procédural. Promulguant les principes essentiels de procédure judiciaire devant être respectés, les législateurs fédéral et cantonal édictent le droit procédural en concrétisant le droit constitutionnel (art. 36 al. 1 et 2 Cst).

b. Les droits garantis

i. La Constitution et les droits fondamentaux en général

217 A l'image de certaines Constitutions cantonales, la Constitution fédérale renferme un catalogue détaillé des droits fondamentaux (art. 7 à 36 Cst). Auparavant garantis par le principe non-écrit de la liberté personnelle, les droits fondamentaux qui nous intéressent en droit de la preuve sont scindés en trois articles: la dignité humaine (art. 7 Cst), le droit à la vie et la liberté personnelle (art. 10 Cst) et la protection de la sphère privée (art. 13 Cst)[217].

---

[215] AUBERT, p. 5; RHINOW, SCHEFER, p. 3.

[216] AUER, HOTTELIER, MALINVERNI, Vol. I, p. 478-479; MASTRONARDI, p. 233; MOOR, FLÜCKIGER, p. 214-215; RHINOW, SCHEFER, p. 10-15.

[217] ATF 107 Ia 148, 150 = JdT 1982 IV 86, 86-87; ATF 109 Ia 146, 155; ATF 113 Ia 257, 265; ATF 122 I 360, 362 = JdT 1998 I 203, 204; ATF 133 I 77, 80; ATF 138 I 256, 258.

218 La dignité humaine représente le droit supérieur des droits fondamentaux permettant de respecter et de protéger les hommes[218]. Pour le Conseil fédéral, le respect de la dignité humaine se décrit comme un "*principe directeur de toute activité étatique*"[219] ou "*tragendes Konstitutionsprinzip*"[220]. Les articles 10 et 13 Cst concrétisent des aspects particuliers de la dignité humaine de sorte que la portée propre de l'art. 7 Cst est restreinte.

219 L'art. 10 Cst garantit le droit à la vie, l'intégrité corporelle et psychique, la liberté de mouvement et l'interdiction de la torture et des peines ou traitements cruels, inhumains ou dégradants[221].

220 La protection de la sphère privée énoncée à l'art. 13 Cst est à la fois une garantie autonome et complémentaire de l'art. 10 Cst. L'alinéa premier garantit le droit au respect de la vie privée, de la vie familiale et du domicile, ainsi que le secret de la correspondance et des télécommunications; le second alinéa vient y ajouter la protection des données personnelles[222].

221 L'art. 36 Cst complète la liste des dispositions constitutionnelles topiques lors de l'application des droits fondamentaux en matière de droit de la preuve. Cette base légale prévoit que "*[t]oute restriction d'un droit fondamental doit être fondée sur une base légale [...] être justifiée par un intérêt public [...] être proportionnée au but visé [et ne peut pas toucher] l'essence des droits fondamentaux.*". Elle reprend ainsi l'exigence générale d'intérêt public et de proportionnalité qui vaut pour toute activité étatique en vertu de l'art. 5 al. 2 Cst.

ii. La Constitution et les garanties procédurales

222 Les art. 29 et 32 Cst renferment les garanties essentielles, minimales et subsidiaires – le droit ordinaire fédéral ou cantonal pouvant être plus strict – de procédure[223]. A l'instar des instruments internationaux, les principes régissant l'administration de la preuve,

[218] JEANNERET, KÜHN, p. 38; MASTRONARDI, p. 239; MÜLLER, SCHEFER, p. 1; RHINOW, SCHEFER, p. 29 et 31-32.

[219] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 144; HÄFELIN, HALLER, KELLER, p. 112; MASTRONARDI, p. 238-239; RHINOW, SCHEFER, p. 30-31.

[220] GRISEL E., p. 61; HÄFELIN, HALLER, KELLER, p. 112; KLEY, p. 325; Message, Constitution, p. 142.

[221] A ce sujet, voir: Infra Partie I, Chapitre 3, III, B, n° 297-299 et 300 ss; Infra Partie II, Chapitre 2, I, B, 1, a, n° 562; Infra Partie II, Chapitre 2, II, B, 1, a, i, n° 846-849; Infra Partie II, Chapitre 3, I, A, 2, a, i, n° 1116-1120; Infra Partie II, Chapitre 3, I, B, 2, a, i, a)-c) , n° 1452-1465; Infra Partie II, Chapitre 3, II, C, 1, n° 1714 et 1717 ss; Infra Partie II, Chapitre 3, III, A, 3, a, n° 1934-1935.

[222] A ce sujet, voir: Infra Partie II, Chapitre 2, I, B, 1, a, n° 562; Infra Partie II, Chapitre 2, II, B, 1, a, ii, n° 852; Infra Partie II, Chapitre 3, I, B, 2, a, i, c) , n° 1463; Infra Partie II, Chapitre 3, III, A, 3, a, n° 1934.

[223] HÄFELIN, HALLER, KELLER, p. 258; HÄNER, p. 21; MÜLLER, SCHEFER, p. 817; RHINOW, SCHEFER, p. 600.

l'appréciation des preuves et leur légalité découlent implicitement de la présomption d'innocence (art. 32 al. 1 Cst), du droit d'être entendu (art. 29 al. 2 Cst renforcé par l'art. 32 al. 2 Cst), de la dignité humaine (art. 7 Cst), du droit à la liberté personnelle (art. 10 al. 2 Cst) et de la protection de la sphère privée (art. 13 Cst).

223 Tout procès équitable (art. 29 al. 1 Cst) doit respecter la présomption d'innocence (art. 32 al. 1 CPP). A la lecture de la jurisprudence[224] et de la doctrine[225], la présomption d'innocence pose les bases du droit de la preuve, puisqu'elle implique deux règles à respecter: le fardeau de la preuve et l'appréciation des preuves.

224 En outre, le droit d'être entendu (art. 29 al. 2 Cst) et de consulter le dossier est concrétisé dans le cadre de la procédure pénale par la reconnaissance des droits de la défense (art. 32 al. 2 Cst)[226]. Dans plusieurs arrêts de jurisprudence constante – en accord avec la doctrine[227] –, le Tribunal fédéral a admis un certain nombre de garanties liées à la preuve: le droit de garder le silence[228], le droit d'administrer des preuves[229], d'interroger les témoins et/ou les experts[230] et le droit de consulter le dossier[231].

225 Concernant la restriction des droits fondamentaux au sens de l'art. 36 Cst, pour reprendre les termes du Conseil fédéral "*[l]e régime défini dans cet article n'est pas applicable à l'ensemble des droits fondamentaux, mais il est essentiellement taillé pour les libertés individuelles [...]. En revanche, le régime des restrictions n'est pas conçu ni adéquat pour [...] certaines garanties de procédure [...]*"[232]. La doctrine s'accorde sur l'inapplicabilité de l'art. 36 Cst aux *Mitwirkungsrechte*[233] dont font notamment partie les art. 29 à 32 Cst.

---

[224] ATF 120 Ia 31, 35-37 = JdT 1996 IV 79 = SJ 1994 541; ATF 130 I 126, 128; ATF 131 I 272, 278; ATF 137 IV 219, 227.

[225] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 621-622; HÄNER, p. 22; JEANNERET, KÜHN, p. 73; MÜLLER, SCHEFER, p. 981-987; TRECHSEL, Human Rights, p. 167; VERNIORY, p. 12. Infra Partie I, Chapitre 3, III, A, n° 285 ss.

[226] HÄFELIN, HALLER, KELLER, p. 276; JEANNERET, KÜHN, p. 51-52; MÜLLER, SCHEFER, p. 993-994; RHINOW, SCHEFER, p. 600.

[227] HÄNER, p. 23; CR-CPP-MACALUSO, art. 113 N 3; MÜLLER, SCHEFER, p. 984; PIQUEREZ, Traité de procédure pénale suisse, p. 273; TRECHSEL, Human Rights, p. 166. Infra Partie I, Chapitre 2, II, A, 2, a, n° 236-237.

[228] ATF 109 Ia 166, 167-168 = JdT 1984 IV 126; ATF 121 II 257, 264; ATF 121 II 273, 281; ATF 130 I 126, 128; JEANNERET, KÜHN, p. 52 ; Preuve-BRENCI, p. 25.

[229] ATF 109 Ia 3; ATF 122 I 53, 55; ATF 128 III 411, 413; HÄFELIN, HALLER, KELLER, p. 261; HÄNER, p. 27; JEANNERET, KÜHN, p. 67; Preuve-BRENCI, p. 24.

[230] ATF 125 I 127, 133; ATF 131 I 476, 481; GRABENWARTER, PABEL, p. 452; HÄNER, p. 24; HARRIS, O'BOYLE, WARBRICK, p. 322; Preuve-BRENCI, p. 24.

[231] ATF 53 I 107, 113; ATF 121 I 225, 228; ATF 129 I 249, 254-255; ATF 132 II 485, 495; CR-CPP-CHAPUIS, art. 101 N 1; HÄFELIN, HALLER, KELLER, p. 262 et 277; JEANNERET, KÜHN, p. 59; MÜLLER, SCHEFER, p. 871 ss; SCHMID, Praxiskommentar, art. 101 N 1.

[232] Message, Constitution, p. 196.

226 Néanmoins, le Tribunal fédéral observe une définition large du mot *restriction* et applique – au moins partiellement – par analogie le régime prévu à l'art. 36 Cst aux garanties des art. 29 à 32 Cst[234]. Par exemple, le droit d'être entendu ne comprend pas le droit à l'oralité ce qui restreint l'exercice de ce droit fondamental[235]. Ainsi, la méthode traditionnelle de restriction n'est pas applicable au *Mitwirkungsrechte*, mais l'emploi par analogie de l'art. 36 Cst ou la délimitation du champ de protection aboutit à la même conclusion.

c. Le champ d'application

227 La Constitution fédérale suisse ne fait pas exception aux instruments internationaux, le principe de non-discrimination (art. 8 Cst) implique un champ d'application personnel large. Les textes des articles 7, 10, 13, 29 et 32 Cst confirment l'égalité de traitement puisqu'ils s'appliquent à "*Toute personne*" ou "*Tout être humain*", soit à toutes les personnes physiques indépendamment de leur nationalité, race, sexe, etc. [236].

228 Matériellement, les champs d'application de la dignité humaine, de la liberté et de la protection de la sphère privée n'amènent pas grand débat. Toutes les libertés élémentaires dont l'exercice est indispensable à l'épanouissement de la personne humaine et le droit d'organiser sa vie ainsi que d'entretenir des rapports avec l'extérieur sont inclus dans la protection des articles 10 et 13 Cst. Autrement dit, le champ d'application matériel de ces deux articles est étendu, d'autant que la liberté personnelle est un droit inaliénable et imprescriptible[237].

229 De plus, tout traitement d'un être humain n'entrant pas dans le champ de protection de ces dispositions peut être appréhendé par l'art. 7 Cst. La garantie de la dignité humaine élargit le champ d'application des droits protégés et inhérents à toute personne, puisque sa portée commence là où s'arrête celle des garanties spécifiques[238].

---

[233] ATF 127 I 54, 56 = JdT 2004 IV 96, 97; ATF 135 I 187, 190; ATF 136 I 265, 272; BELSER, WALDMANN, MOLINARI, p. 142; HÄFELIN, HALLER, KELLER, p. 279; MÜLLER, SCHEFER, p. 871 ss.

[234] ATF 129 I 12, 20-27 = JdT 2004 I 9, 16-23; ATF 135 II 243, 248; ATF 136 I 197, 205; HÄFELIN, HALLER, KELLER, p. 280; MÜLLER, p. 639.

[235] ATF 108 Ia 188, 192; ATF 122 II 464, 469; ATF 125 I 209, 219; ATF 130 II 425, 428; ATF 134 I 140, 148; ATF 136 V 117, 126-127.

[236] AUBERT, MAHON, art. 13 N 4; BELSER, WALDMANN, MOLINARI, p. 80; GRISEL E., p. 6; SCHWEIZER R., p. 696.

[237] AUBERT, MAHON, art. 10 N 7; GRISEL E., p. 83-84; MÜLLER, SCHEFER, p. 45.

[238] AUBERT, MAHON, art. 7 N 4; GRISEL E., p. 61; HÄFELIN, HALLER, KELLER, p. 112; JEANNERET, KÜHN, p. 38.

230 Les garanties de procédure en matière pénale ont un champ d'application plus restrictif. Elles n'appartiennent qu'aux personnes poursuivies ou prévenues d'une infraction pénale. Le terme "*accusé*" doit s'interpréter largement, il englobe toute personne à partir du moment où elle s'est vue reprocher, par un organe de l'Etat, la commission d'une infraction[239]. Ainsi, le droit d'être entendu – plus particulièrement le droit de participer à l'administration des preuves – et la présomption d'innocence – de manière extensive le droit au silence – est garanti à toute personne partie à une procédure, de la phase d'instruction à la clôture du délai ou des voies de recours.

2. Les lois fédérales

231 Hiérarchiquement, les lois fédérales sont dans un rapport d'infériorité avec la Constitution. Les objets réglementés dans les lois sont divers et variés mais limités par le caractère impératif du cadre constitutionnel. Néanmoins, elles occupent une place privilégiée dans notre système juridique

a. Le Code de procédure pénale suisse – CPP

232 Le 5 octobre 2007, le Conseil fédéral a adopté le Code de procédure pénale mettant un terme à treize années de travaux préparatoires. Cette loi est entrée en vigueur le 1er janvier 2011 obligeant les cantons – pour la première fois – à appliquer un droit de procédure formel et unifié au plan national.

233 Constituant une nouveauté concernant le champ d'application territorial, le Code de procédure pénale l'est également dans certains domaines principalement par l'intégration de normes relevant d'autres lois fédérales et reprises de manière quasi identique[240].

234 Structurellement, le CPP est divisé en douze titres réglementant chacun une facette de la procédure pénale. Le premier est applicable à l'ensemble des autres titres. Pour le surplus, chaque titre débute par des dispositions générales applicables à l'ensemble de son contenu et se complète par des dispositions spécifiques à certaines circonstances.

---

[239] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 624; HOTTELIER, Garanties de procédure, p. 812; MÜLLER, SCHEFER, p. 980; VERNIORY, p. 70.

[240] Art. 3 al. 1, 3 al. 2, 5 et 7 Loi sur les profils d'ADN correspondent respectivement aux art. 255 al.1 let. a et b, 256, 257 et 255 al. 2 CPP; Art. 3, 4, 8 al. 1-2 et 9 LSCPT sont quasiment identiques aux art. 269, 270-271, 276 et 278 CPP.

235 Au point de vue matériel, le champ d'application exclut à l'évidence la poursuite et le jugement d'infractions réprimées par le droit cantonal (art. 1 al. 1 CPP). Une réserve est toutefois réalisée sur l'applicabilité des dispositions procédurales spécifiques découlant d'autres lois fédérales (art. 1 al. 2 CPP)[241]. Ainsi, le CPP couvre les procédures pénales relatives aux adultes – exception faite des personnes visées par la procédure pénale militaire[242] – et aux mineurs (art. 3 PPMin). En revanche, la violation du droit international est passée sous silence quant à l'applicabilité du CPP. Vraisemblablement, le CPP doit pouvoir s'appliquer dans les cas où le droit international ne prévoit pas de juridiction internationale[243].

236 En ce qui concerne les droits garantis s'intégrant dans le cadre du droit de la preuve, notre intérêt se porte, nous le verrons, sur les dispositions du Titre 1 Chapitres 2 et 7, du Titre 4, ainsi qu'à certains chapitres du Titre 5. Le contenu des art. 3 à 11 CPP reprend – de manière non-exhaustive – la plupart des concepts et des droits fondamentaux – dignité humaine, procès équitable, indépendance du tribunal, présomption d'innocence, etc. – institués dans les instruments universels, régionaux et dans la Constitution fédérale[244].

237 Concernant le droit d'être entendu, il nous faut relever que le Code de procédure pénale concrétise spécifiquement cette notion[245]. L'art. 107 CPP précise que cette garantie accordée à l'accusé lui permet de"*[…]; a. consulter le dossier; b. participer à des actes de procédure; d. se prononcer au sujet de la cause et de la procédure; e. déposer des propositions relatives aux moyens de preuves.*". En outre, les parties peuvent consulter toutes les pièces du dossier les concernant, ainsi que le dossier des co-prévenus, ceci "*[…] au plus tard après la première*

[241] Loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA), RS 313.0; Procédure pénale militaire du 23 mars 1979 (PPM), RS 322.1, ainsi que les dispositions particulières de la loi sur la procédure pénale applicable aux mineurs (Procédure pénale applicable aux mineurs, PPMin), RS 312.1, de la loi fédérale du 24 juin sur les amendes d'ordre (LAO), RS 741.03, et de la loi fédérale du 17 juin 2005 sur le Tribunal fédéral (LTF), RS 173.110, lorsque le Tribunal fédéral agit en qualité d'autorité de recours.

[242] Code pénal militaire du 13 juin 1927 (CPM), RS 321.0.

[243] CR-CPP-ARN, STEINER, art. 1 N 16; VERNIORY, p. 93.

[244] Supra Partie I, Chapitre 2, I, A, 1, b, n° 171-172 et 174-175; Supra Partie I, Chapitre 2, I, A, 2, b, n° 182 et 185-189; Supra Partie I, Chapitre 2, I, B, 1, b, n° 196 et 198; Supra Partie I, Chapitre 2, II, A, 1, b, ii, n° 222.

[245] CourEDH, Affaire *Colozza c. Italie*, arrêt du 12 février 1985, 9024/80, § 27; CourEDH, Affaire *Feldbrugge c. Pays-Bas*, arrêt du 29 mai 1986, 8562/79, § 44; CourEDH, Affaire *Barberà, Messegué et Jabardo c. Espagne*, arrêt du 6 décembre 1988, 10590/83, § 83; CourEDH, Affaire *Murray c. Royaume-Uni*, arrêt du 8 février 1996, 18731/91, § 45; CourEDH, Affaire *Werner c. Autriche*, arrêt du 24 novembre 1997, 21835/93, § 45; CourEDH, Affaire *Pisano c. Italie*, arrêt du 27 juillet 2000, 36732/97, § 21; CourEDH, Affaire *Medenica c. Suisse*, arrêt du 14 juin 2001, 20491/92, § 54; OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *Observation générale n° 13: L'égalité devant les tribunaux et le droit d'être entendu équitablement et publiquement par un tribunal indépendant et établi par la loi (art. 14)*, Genève 1984, disponible sur: http://www.unhchr.ch [consulté le 08.05.2016], § 12; JEANNERET, KÜHN, p. 52; MEUNIER, p. 192; RHINOW, SCHEFER, p. 600; SCHMID, Praxiskommentar, art. 107 N 1; StPO-LIEBER, art. 107 N 2.

audition du prévenu et l'administration des preuves principales par le ministère public […]" (art. 101 CPP).

238 D'autres précisions sont apportées par les dispositions du CPP. L'art. 10 CPP concrétise la présomption d'innocence (10 al. 1 et 3 CPP) et prévoit explicitement la libre appréciation des preuves devant mener à l'intime conviction (art. 10 al. 2 CPP)[246]. La recherche de la vérité matérielle et son corollaire, l'administration d'office des preuves (art. 6 CPP), sont le point d'ancrage de la conviction du juge[247].

b. Les législations fédérales complémentaires

239 L'appellation "*législations fédérales complémentaires*" regroupe la loi sur la protection des données (i.), la loi sur l'utilisation de profils d'ADN dans la procédure pénale et sur l'identification de personnes inconnues ou disparues (ii.), la loi sur la surveillance de la correspondance par poste et télécommunication (iii.) et la loi sur les systèmes d'information de police de la Confédération (iv.).

240 Ces actes normatifs fédéraux ne formulent pas clairement le droit de la preuve, mais tous renferment des éléments indispensables – garanties fondamentales, procédure de recueil, d'utilisation, de conservation et d'administration – à l'appréhension des nouvelles technologies comme moyens de preuves.

i. La loi sur la protection des données – LPD

241 L'avènement de l'informatique et des technologies de télécommunications, du traitement automatisé de données ainsi que l'augmentation du nombre d'informations personnelles diffusées ont accru les risques de violation des droits fondamentaux, particulièrement de la sphère privée. La LPD a pour mission principale de remédier aux lacunes des législations en vigueur et d'offrir une protection efficace aux personnes concernées par les traitements de données (art. 1 LPD)[248].

[246] ATF 120 Ia 31, 36-37 = JdT 1996 IV 79 = SJ 1994 541; ATF 127 I 38, 40-41.

[247] Infra Partie I, Chapitre 3, II et III, n° 281 ss et 287-288.

[248] Message, LPD, p. 424-425.

242 La LPD trouve application dans tous les traitements de données concernant les personnes physiques ou morales par des personnes privées ou par des organes fédéraux (art. 2 al. 1 LPD).

243 Du point de vue matériel, l'applicabilité ne vaut – en règle générale – pas pour les traitements de données personnelles effectués par les autorités cantonales. Toutefois, l'art. 37 al. 1 LPD instaure une norme supplétive fixant une protection minimale en cas de traitement par des organes cantonaux ne disposant pas d'une protection adéquate, soit au moins équivalent à celle qui prévaut pour la Convention STE n°108 (art. 5 à 11).

244 De surcroît, le champ d'application de la loi sur la protection des données est limité par l'art. 2 al. 2 LPD. La LPD ne s'applique notamment pas lors de procédures pénales pendantes (art. 2 al. 2 let. c). Lors d'un traitement de données d'un suspect, la procédure pénale n'étant pas encore pendante, la LPD est applicable. Lorsque le suspect devient un prévenu, les normes du CPP relatives à ce domaine prennent le relais. Pour finir, lorsque le prévenu bénéficie d'un classement, lorsqu'il est acquitté ou encore lorsqu'une décision de culpabilité est rendue et après extinction du délai de recours, le traitement des données personnelles récoltées durant l'enquête est à nouveau protégé par la LPD[249].

245 Quant au champ d'application personnel, l'art. 2 al. 1 LPD garantit une protection tant aux personnes physiques qu'aux personnes morales.

246 Globalement, la LPD concrétise la protection de la personnalité (art. 8 CEDH, art. 17 Pacte II, art. 10 et 1 Cst et art. 12 DUDH) s'agissant des échanges d'informations, des traitements de ses données personnelles et de leur conservation.

ii. La loi sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues – Loi sur les profils d'ADN

247 Faisant suite au message du Conseil fédéral du 8 novembre 2000, le Parlement arrête, le 20 juin 2003, la loi fédérale sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (Loi sur les profils d'ADN) avec mise en vigueur le 1er janvier 2005.

[249] DSG-WALDMANN, BICKEL, p. 661-662; Message, Convention à l'égard du traitement automatisé, p. 709-710; MEIER P., p. 190; ROSENTHAL, JÖHRI, art. 2 N 32.

248 L'utilisation des données génétiques comprend deux étapes que la présente loi différencie: d'une part, la phase de prélèvement et traitement d'échantillons, d'autre part – celle de saisie dans un système d'information et d'exploitation de profils d'ADN. Structurellement, cette différenciation est constatable grâce à la scission par sections des diverses dispositions légales. Les sections 2 et 3 de la loi règlent la phase d'utilisation d'échantillons – champs d'application matériel et personnel, conditions à respecter pour prélever, analyser et conserver un échantillon – alors que les sections 4 à 7 régissent de manière similaire les profils d'ADN, exception faite de l'art. 15 Loi sur les profils d'ADN qui consacre un droit dès le prélèvement d'échantillons. Quant à la première et la dernière des sections, elles s'appliquent tant à la première qu'à la deuxième étape des analyses génétiques.

249 La loi sur les profils d'ADN garantit, dans le cadre particulier des analyses et de l'établissement de profils génétiques, la dignité humaine, la liberté personnelle, la protection de la sphère privée et le droit à l'autodétermination informationnelle et applique certaines garanties de la LPD[250].

250 D'un point de vue personnel, le prélèvement et l'établissement d'un profil d'ADN concernent les personnes suspectées d'avoir commis un crime ou un délit (art. 3 al. 1 let. a et art. 11 al. 1 let. a Loi sur les profils d'ADN), les autres personnes liées de près à l'infraction comme la victime (art. 3 al. 1 let. b et art. 11 al. 1 let. a Loi sur les profils d'ADN), les personnes décédées et les traces (art. 4 et 11 al. 1 let. c Loi sur les profils d'ADN), les personnes condamnées (art. 5 et 11 al. 1 let. b Loi sur les profils d'ADN), ainsi que toutes les personnes citées à l'art. 6 Loi sur les profils d'ADN quand l'identification a lieu hors de la procédure pénale, soit: les personnes vivantes ou décédées non identifiées (art. 6 al. 1-2 et 11 al. 2 let. a Loi sur les profils d'ADN), les matériels biologiques des personnes disparues (art. 6 al. 3 et 11 al. 2 let. b Loi sur les profils d'ADN) ou les parents des personnes décédées ou disparues qui doivent être identifiées (art. 6 al. 4 et 11 al. 2 let. c Loi sur les profils d'ADN).

251 Au point de vue matériel, le recours au prélèvement et à l'analyse d'ADN doit permettre d'identifier les suspects ou de lever les soupçons contre eux, de relier des infractions entre elles et de contribuer à l'administration des preuves (art. 1 al. 2 Loi sur les profils d'ADN). Le champ d'application est complété par l'identification des personnes inconnues, disparues ou décédées (art. 1 al. 3 Loi sur les profils d'ADN).

252 Lorsque le profilage ADN est effectué dans le cadre d'une procédure pénale, le champ d'application matériel de l'art. 1 Loi sur les profils d'ADN est réduit par une série de

[250] Message, ADN, p. 23-24 et 29. Infra Partie II, Chapitre 2, II, B, 1, a, n° 562.

conditions propres à chaque phase de la procédure d'analyse génétique. Le prélèvement d'échantillon ADN est autorisé aux fins d'élucider un crime ou un délit (art. 3 al. 1 et 4 *in fine* Loi sur les profils d'ADN), ce qui exclut l'identification de l'auteur d'une contravention.

253 Dans l'hypothèse où l'infraction a préalablement été élucidée, un échantillon d'ADN peut être prélevé lorsqu'un jugement condamnatoire est entré en force (art. 5 Loi sur les profils d'ADN) et qu'il concerne une infraction de commission intentionnelle punie d'une peine effective d'un an de privation de liberté au minimum ou concerne un acte délictuel lésant la vie, l'intégrité corporelle, voire l'intégrité sexuelle (art. 5 let. a et b Loi sur les profils d'ADN). Les personnes contre lesquelles une mesure est prononcée peuvent aussi faire l'objet d'une analyse génétique (art. 5 let. c Loi sur les profils d'ADN).

254 Notons toutefois que lorsque la procédure pénale est régie par le CPP, la Loi sur les profils d'ADN n'est pas applicable (art. 1a Loi sur les profils d'ADN). Globalement similaire aux articles 1, 3 al. 1-2 et 5 Loi sur les profils d'ADN, les articles du CPP adaptent la réglementation sur le prélèvement d'échantillons et l'établissement de profils d'ADN à la stricte procédure pénale fédérale, sans pour autant dénuer la loi du 20 juin 2003 de toute utilité. Cette dernière continue de régir la procédure ne tombant pas sous le coup des articles du CPP ainsi que la saisie des profils d'ADN dans un fichier automatisé (art. 259 CPP)[251].

255 Au surplus, la seconde partie de notre travail traitant de la preuve génétique, les dispositions légales du CPP et de la Loi sur les profils d'ADN seront objectivées[252].

iii. La loi sur la surveillance de la correspondance par poste et télécommunication – LSCPT[253]

256 Le Parlement arrête le 6 octobre 2000 la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Depuis le 1er janvier 2002, cette loi est entrée en vigueur.

257 La procédure et les conditions à respecter prévues dans cette loi concernent deux types de surveillances, celle de la correspondance par poste et celle des télécommunications (art. 1 LSCPT). Contrairement à la surveillance du courrier postal, le second dispositif intègre, en partie, les nouvelles technologies qui nous intéressent.

---

[251] Message, CPP, p. 1223. Infra Partie II, Chapitre 2, II, B, 1, b, ii-iii, n° 886 ss et 893 ss.

[252] Infra Partie II, Chapitre 2, II, B, 1, b, n° 861 ss.

[253] Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT), RS 780.1.

258 A l'instar de la loi sur les profils d'ADN, le CPP a repris partiellement les dispositions de la LSCPT aux articles 269 ss CPP. La deuxième partie de notre travail mettant en exergue la procédure de surveillance des télécommunications en lien avec la téléphonie fixe et mobile, l'Internet ainsi que leur utilisation comme moyens probatoires, le développement des dispositions contenues dans le CPP, la loi et son ordonnance suivra[254].

259 Notons encore que cette loi a été révisée en date du 18 mars 2016 avec un délai référendaire au 7 juillet 2016[255]. La révision de la LSCPT vise à ce que les surveillances par poste et télécommunication ne soient pas mises en échec par l'utilisation de nouvelles technologies, notamment la téléphonie par Internet (cryptée). Ainsi, principalement, l'objectif est d'adapter tant la LSCPT que les dispositions idoines du CPP à l'évolution technologique et aux développements futurs prévisibles, notamment les IMSI-catchers (introduction de l'art. 269*bis* CPP) ou les programmes Govware (introduction de l'art. 269*ter* CPP)[256].

iv. La loi sur les systèmes d'information de police de la Confédération – LSIP[257]

260 L'Office fédéral de la police – fedpol – assume la responsabilité de divers systèmes informatiques: le système RIPOL concernant les recherches informatisées de la police, le système AFIS sur les empreintes digitales, le système fondé sur les profils d'ADN, le système IPAS consacré à la gestion et l'indexation de dossiers et de personnes, le système JANUS sur les données de la police judiciaire fédérale traitées dans le cadre de procédures d'enquêtes ou d'investigations préliminaires, etc.[258].

261 La mise en œuvre des systèmes d'information n'est pas sans importance pour l'accomplissement des tâches de poursuite pénale, de police et de maintien de la sécurité. Le développement des bases de données a poussé le Conseil fédéral à élaborer un projet de loi sur les systèmes d'information de la police de la Confédération (LSIP). Cette loi a pour objectif, notamment, de rassembler et d'actualiser les fondements légaux de trois systèmes de police existants: RIPOL, IPAS, JANUS, pour permettre une meilleure transparence et une meilleure circulation des informations recueillies lors d'enquêtes et de procédures pénales[259].

---

[254] Infra Partie II, Chapitre 3, I, A, 2, c, n° 1140 ss.

[255] FF 2016 p. 1821.

[256] Message, P-LSCPT, p. 2381.

[257] Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP), RS 361.0.

[258] Message, LSIP, p. 4822.

[259] Message, LSIP, p. 4823-4824.

262 Concernant les bases de données fédérales n'entrant pas dans le champ d'application de l'art. 2 let. a LSIP, leur légitimation découle de lois ou d'ordonnances spécifiques.

263 Dans le cadre de la LSIP, les autorités fédérales de police sont habilitées à traiter des données sensibles, voire des profils de la personnalité, et à les communiquer aux organes de police et de poursuite pénale cantonales ou aux autres autorités suisses et étrangères (art. 3 al. 2 LSIP).

B. Le droit cantonal

264 Outre les Constitutions cantonales (1.), les cantons édictent des lois relatives à la protection des données personnelles ou encore réglementent les tâches de la police (2.).

1. Les Constitutions cantonales

265 L'obligation de se doter d'une Constitution cantonale écrite découle de l'art. 51 Cst. Parmi les règles constitutionnelles cantonales, les droits fondamentaux occupent une place privilégiée.

266 Jusqu'en 1963, les Constitutions cantonales avaient une importance non négligeable en garantissant les libertés individuelles[260]. Depuis leur concrétisation dans la jurisprudence du Tribunal fédéral, puis des art. 7 ss Cst, les garanties cantonales ont perdu de leur importance ne devenant plus qu'une source subsidiaire de protection[261]. Le Tribunal fédéral reconnaît une portée propre aux garanties fondamentales du droit cantonal dans l'unique hypothèse où elles sont plus précises et offrent une protection plus étendue que les bases légales fédérales ou internationales[262].

267 En matière pénale, la mention des garanties de procédure n'est pas uniformisée dans les vingt-six Constitutions cantonales. Seuls neuf cantons[263] réglementent la totalité des garanties et droits liés à la preuve – procès équitable, juge indépendant et impartial, présomption d'innocence, droit d'être entendu et consultation du dossier – parfois implicitement avec la notion unique d'"*équité*" ou de "*droit de la défense*". Onze Constitutions

[260] AUBERT, MAHON, art. 10 N 1; AUER, HOTTELIER, MALINVERNI, Vol. II, p. 146; HÄFELIN, HALLER, KELLER, p. 74-76.

[261] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 39-40; GRISEL E., p. 2; HÄFELIN, HALLER, KELLER, p. 74-76.

[262] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 38; BELSER, WALDMANN, MOLINARI, p. 64; GRISEL E., p. 2.

[263] art. 20 Cst/AR; art. 26 al. 1 Cst/BE; art. 32 al. 1 et 2 Cst/FR; art. 28, 29 et 31 al. 1 Cst/NE; art. 4 Cst/SG; art. 18 al. Cst/SH; art. 10 al. 2 Cst/TI; art. 27 à 29 Cst/VD.

cantonales[264] font référence à une ou plusieurs garanties: droit d'être entendu, droit d'accès au dossier ou présomption d'innocence; trois d'entre elles exposent les préceptes généraux applicables à la procédure de perquisition. Quatre Etats fédérés[265] se sont bornés à introduire un renvoi à la Constitution fédérale et aux instruments internationaux, voire aux réglementations sur la procédure pénale. Deux Constitutions[266] sont muettes tant au sujet du droit de la preuve que du droit de la défense ou des garanties de procédure. La diversité normative n'est cependant pas un problème étant donné que le Code de procédure pénale relègue à un rôle purement déclaratif les Constitutions cantonales dès lors qu'il met en œuvre de manière concrète et avec précision le droit de la preuve.

268 Ce dernier constat implique que dans le cadre de notre recherche, l'étude des dispositions constitutionnelles cantonales ne sera pas développée.

2. Les législations complémentaires

269 Certaines compétences sont laissées aux cantons. Ainsi, les lois cantonales, les décrets, les règlements d'application ou les ordonnances sont des sources de droit procédural.

270 Au vu du nombre de dispositions concernées par le droit de la preuve, de la protection des données et de la réglementation relative à l'emploi des nouvelles technologies, une présentation des bases légales contenues dans les normes cantonales aurait généré des répétitions et des confusions.

271 Les champs d'application matériels et personnels, ainsi que les droits garantis n'amènent guère de commentaires qui n'ont pas déjà été faits. Selon les domaines, le champ d'application personnel est plus ou moins large. Parfois, toutes les personnes physiques bénéficient des garanties[267], alors que d'autres fois seuls les suspects ou prévenus sont les bénéficiaires d'une garantie[268].

272 Les droits garantis sont, quant à eux, similaires aux garanties contenues dans les législations fédérales, tout en précisant ou complétant un domaine peu ou pas réglé par ces dernières.

---

[264] art. 22 al. 1 Cst/AG; art. 9 al. 3 Cst/BL; art. 4 et 23 Cst/GE et art. 40 nCst/GE; art. 12 al. 2 phr. 2 et 16 al. 5 Cst/GL; art. 9 al. 2 et 3 Cst/JU; art. 3 al. 2 et 4 Cst/NW; art. 11 al. 3 et 12 Cst/OW; art. 18 al. 2 Cst/SO; art. 14 al. 1 et 2 Cst/TG; art. 13 al. 2 Cst/UR; art. 8 al. 2 Cst/ZG.

[265] art. 45 Cst/AI; art. 8 Cst/GR; art. 10 al. 2 Cst/LU; art. 10 al. 1 Cst/ZH.

[266] Cst/SZ et Cst/VS.

[267] A ce sujet, voir: les lois cantonales sur la protection des données, notamment la LIPAD/GE.

[268] A ce sujet, voir: notamment, les diverses loi sur la police cantonale, notamment la LPol/GE.

Prenons l'exemple de la LPD, cette loi ne réglemente pas le traitement des données par les organes cantonaux. La compétence d'édicter une législation cantonale de protection des données revient à chacun des Etats fédérés. Les cantons ayant rédigé récemment une norme en la matière ont largement repris les principes généraux contenus dans la LPD[269]. Conséquemment, la seule réelle différence entre la loi fédérale et les législations cantonales est l'organe concerné par l'application des dispositions. Dans l'accomplissement de leurs tâches, les autorités policières et judiciaires cantonales sont soumises à la procédure et au droit de protection des données propre à leur canton et ce même si elles exécutent un traitement de droit fédéral.

273 Pour plus de détails, nous renvoyons aux divers chapitres sur les preuves qui traitent notamment de la LIPAD/GE[270] et, implicitement, des législations cantonales sur la police.

[269] Message, Convention à l'égard du traitement automatisé, p. 706.

[270] Loi cantonale genevoise du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD), RS/GE 2 08.

CHAPITRE 3: LA PREUVE – PRÉSENTATION GÉNÉRALE

274 La procédure pénale préliminaire, s'étendant de l'enquête à l'instruction, est dominée par la recherche probatoire, la détermination objective et subjective des faits, l'appréciation des preuves et le constat du ministère public qui ordonne le classement (art. 319 ss CPP) ou engage l'accusation (art. 324 ss CPP). Au cours du procès, la preuve est centrale pour la recherche de la vérité matérielle.

275 Les moyens de preuves à disposition des autorités pénales étant variés, des dispositions légales propres à chacun sont édictées. Néanmoins, des principes généraux existent: quels éléments doit-on prouver? (I.), que doit-on rechercher? (II.), à qui revient le fardeau de la preuve? (III. A.), quels moyens de preuves peuvent être administrés? (III. B et IV.), jusqu'où faut-il prouver? (III. C.)

I. L'objet de la preuve

276 Pour que le juge puisse statuer sur la culpabilité ou l'innocence d'un accusé, il est nécessaire d'établir qu'une infraction pénale a été commise par l'accusé. La preuve a pour but d'élucider et de démontrer les faits constitutifs – objectifs et subjectifs – d'une infraction et/ou d'identifier l'auteur[271].

277 Ainsi, dans le cadre des débats, la partie poursuivante – composée du ministère public (art. 104 al. 1 let. c CPP) et de la partie plaignante (art. 104 al. 1 let. b *cum* 118 al. 1 CPP) – doit apporter la preuve de l'existence des deux éléments qui constituent l'infraction: l'élément matériel soit la démonstration des faits constitutifs d'un action ou d'une omission pénalement répréhensible, l'accomplissement d'éventuelles circonstances aggravantes réelles et l'identification de l'auteur; et l'élément moral qui concerne l'intentionnalité de l'accusé, la double intentionnalité en cas de participation accessoire ou la violation du devoir de prudence en cas d'infraction par négligence[272].

[271] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 115-116; PIETH, p. 161; PITTELOUD, p. 223; RIEDO, FIOLKA, NIGGLI, p. 163; SCHMID, Handbuch, p. 311.

[272] BOULOC, p. 108-110; PIQUEREZ, Traité de procédure pénale suisse, p. 331.

278 Dans le cadre de l'administration de la preuve, la distinction entre le fait juridique et le droit est essentielle[273]. La preuve de l'élément légal, soit l'existence d'une base légale répressive, n'est pas à la charge de l'accusation[274]. Conformément à l'adage du droit romain "*jura novit curia*", le juge connaît le droit qu'il doit interpréter et appliquer lorsqu'il est démontré qu'un auteur a adopté un comportement pénalement répréhensible (art. 1er CP), étant précisé que la tâche du juge relativement à l'objet de la preuve s'arrête à la démonstration de la typicité de l'acte délictueux. Il incombe à la partie poursuivante de démontrer que l'action pénale n'est pas prescrite et à la défense de rendre vraisemblable qu'un élément justificatif ou d'exemption de peine peut être apporté[275].

279 Relevons encore que, dans un but d'économie dans la procédure, tous les faits ne sont pas à établir. Les faits non pertinents, évidents ou notoires, connus de l'autorité pénale ou suffisamment prouvés ne sont pas soumis à l'administration de la preuve (art. 139 al. 2 CPP)[276]. La restriction dans l'administration des preuves intervenant avant que le juge ne puisse se prononcer sur l'affaire, elle doit s'analyser avec prudence et dans le cas concret[277].

II. La recherche de la vérité matérielle

280 "Il n'est de justice que dans la vérité." [Emile Zola]

281 Le point de départ de toute procédure pénale est la recherche de la vérité matérielle[278]. Ce principe est codifié à l'art. 6 al. 1 CPP. Il préconise que l'autorité pénale établisse les faits tels qu'ils se sont réellement déroulés ou, en tout cas, selon une vérité objective et complète qui paraît certaine[279]. Une simple vérité relative ou formelle est insuffisante, selon l'adage *in dubio pro reo*[280].

---

[273] KAUFMANN, p. 5-6.

[274] BOULOC, p. p. 108-110; MOREILLON, PAREIN-REYMOND, art. 6 N 5; PIQUEREZ, Traité de procédure pénale suisse, p. 331 ; Preuve-BOHNET, JEANNERET, p. 67.

[275] PIQUEREZ, Traité de procédure pénale suisse, p. 183.

[276] A ce sujet: JOSITSCH, Strafprozessrechts, p. 88; KAUFMANN, p. 13-14 et 18; MOREILLON, PAREIN-REYMOND, art. 139 N 9; Preuve-BOHNET, JEANNERET, p. 68; RIEDO, FIOLKA, NIGGLI, p. 165; SCHMID, Handbuch, p. 311-312.

[277] Message, CPP, p. 1161; RIEDO, FIOLKA, NIGGLI, p. 165; SCHMID, Handbuch, p. 311.

[278] CR-CPP-ROTH, art. 6 N 5; MOREILLON, PAREIN-REYMOND, art. 6 N 1; RIEDO, FIOLKA, NIGGLI, p. 166; SCHMID, Praxiskommentar, art. 6 N 1; StPO-WOHLERS, art. 6 N 1.

[279] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-MAURER, p. 6; MOREILLON, PAREIN-REYMOND, art. 6 N 3; RIEDO, FIOLKA, NIGGLI, p. 166; RUCKSTUHL, VOLKER, ARNOLD, p. 47; SCHMID, Handbuch, p. 56.

[280] Infra Partie I, Chapitre 3, III, A, n° 285-290; Infra Partie I, Chapitre 3, III, C, 2, n° 317-319.

282 Afin de trouver la vérité matérielle, l'autorité pénale décisionnelle ne peut pas se satisfaire des déclarations des parties ou des preuves. En ce sens, la recherche de la preuve par les autorités étatiques est essentielle en procédure pénale. Elle trouve toute son essence dans les principes d'enquête, d'investigation ou d'instruction (art. 299 ss CPP) et dans le principe de vérité[281].

283 Ainsi, la recherche des preuves par les autorités pénales (art. 6 al. 1 CPP) est confiée à divers organes judiciaires. Toutes les autorités pénales – la police judiciaire et le ministère public durant la procédure préliminaire, les autorités de jugement durant la phase des débats – doivent rechercher d'office les éléments pertinents à charge ou à décharge du prévenu[282]. Pour accomplir leur tâche, les autorités bénéficient de moyens coercitifs – perquisition, saisie, mesure de surveillance, etc. – qui leur permettent de rassembler et d'exploiter des preuves[283].

III. La théorie générale de la preuve

284 Lorsque nous analysons la théorie de la preuve trois questions se posent (art. 10, 139 à 141 CPP). L'application du principe de la présomption d'innocence et de son corollaire, le fardeau de la preuve, répondent à "*Qui doit prouver?*" (A.). L'exposé de la liberté de la preuve et de ses limites résout la question "*Comment prouver?*" (B.). Le principe de la libre appréciation des preuves et de l'intime conviction répondent à "*Jusqu'où faut-il prouver?*" (C.). Comme nous le verrons[284], les réponses aux trois questions ne sont pas indépendantes l'une de l'autre. La présomption d'innocence (art. 10 al. 1 et 3 CPP) est intimement liée au besoin d'atteindre l'intime conviction (art. 10 al. 3 CPP) qui lui-même nécessite l'administration des preuves (art. 139 à 141 CPP).

A. La charge de la preuve et la présomption d'innocence

285 La présomption d'innocence maxime fondamentale de tout procès équitable (art. 6 § 2 CEDH, art. 14 § 2 Pacte II, art. 32 al. 1 Cst et art. 11 § 1 DUDH) est prévue de manière détaillée en procédure pénale (art. 10 al. 1 à 3 CPP).

---

[281] JOSITSCH, Strafprozessrechts, p. 87; RUCKSTUHL, DITTMANN, ARNOLD, p. 47; SCHMID, Praxiskommentar, art. 139-141 N 1-2.

[282] CR-CPP-ROTH, art. 6 N 6; MOREILLON, p. 143; Preuve-BOHNET, JEANNERET, p. 67; SCHMID, Handbuch, p. 56.

[283] PERRIER, VUILLE, p. 17; PIQUEREZ, Traité de procédure pénale suisse, p. 173; Polizeiliche Ermittlung-VOSER, p. 25.

[284] Infra Partie II, Chapitre 3, III, A à C, n° 285 ss.

286 L'art. 10 al. 1 CPP consacre le principe de la présomption d'innocence comme base à tout procès pénal. A l'instar des réglementations internationales et constitutionnelles, il s'adresse à toutes les autorités – organes de police et de justice – et plus particulièrement au juge du fond. En outre, l'art. 10 al. 3 CPP prévoit de manière explicite l'applicabilité de l'adage *in dubio pro reo* obligeant le tribunal à prononcer l'acquittement si un doute subsiste[285].

287 Ainsi, l'innocence est présumée tant qu'aucune preuve n'établit d'un point de vue objectif la culpabilité pénale de l'accusé. *A contrario*, s'il existe un doute, la personne ne peut jamais être reconnue coupable. Le principe de la présomption d'innocence est par conséquent constitué de deux volets: le fardeau de la preuve et la non-culpabilité en cas doute. Stefan Trechsel[286] – notamment – et le Tribunal fédéral[287] déclarent qu'une règle supplémentaire est attachée à la présomption d'innocence, plus spécifiquement au principe *in dubio pro reo*. Il s'agit de l'appréciation des preuves.

288 Résultante des garanties d'un procès équitable et d'un tribunal indépendant et impartial[288], la présomption d'innocence implique que les faits objectifs soient établis en dispensant la personne suspectée ou poursuivie de démontrer son innocence[289]. L'accusé peut donc adopter une attitude passive impliquant le droit de se taire et de ne pas contribuer à sa propre incrimination[290]. Le fardeau de la preuve des faits et de la culpabilité incombe à la partie poursuivante – ministère public et/ou partie plaignante –, voire au juge répressif[291].

289 A la question de savoir quelle est la portée de la présomption d'innocence, l'objet de la preuve fournit la solution. A l'exception de l'accomplissement de la preuve de la vérité (par exemple: art. 173 ch. 2 CP), d'un motif justificatif, d'un motif d'absolution ou d'un motif diminuant la culpabilité, le fardeau de la persuasion repose sur le demandeur. Il importe alors peu que

---

285 CR-CPP-VERNIORY, art. 10 N 47; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 58-60; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-MAURER, p. 11; JEANNERET, KÜHN, p. 74; MOREILLON, PAREIN-REYMOND, art. 10 N 15; PERRIER DEPEURSINGE, art. 10, p. 27 et 29; Preuve-BOHNET, JEANNERET, p. 72; RUCKSTUHL, DITTMANN, ARNOLD, p. 67; SCHMID, Praxiskommentar, art. 10 N 1 et 10; StPO-WOHLERS, art. 10 N 1 et 11-14.

286 TRECHSEL, RSJ, p. 319.

287 ATF 120 Ia 31, 36 = JdT 1996 IV 79 = SJ 1994 541, 543-544; ATF 137 IV 219, 227 = JdT 2012 IV 126, 133.

288 ATF 124 I 327, 331; MOREILLON, PAREIN-REYMOND, art. 10 N 4.

289 ATF 124 IV 86, 87-88 = JdT 1999 IV 136, 137-138; ATF 127 I 38, 40-41 = JdT 2004 IV 65, 67-68; ATF 138 V 74, 81-82; CR-CPP-VERNIORY, art. 10 N 16; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 59; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-MAURER, p. 10; JEANNERET, KÜHN, p. 72-73; StPO-WOHLERS, art. 10 N 1 et 11-14.

290 EICKER, HUBER, p. 115; PIQUEREZ, RJJ 1994, p. 288-289; PIQUEREZ, RJJ 2004, p. 16-17; RUCKSTUHL, DITTMANN, ARNOLD, p. 69.

291 BOULOC, p. 103; CR-CPP-VERNIORY, art. 10 N 45; MERLE, VITU, T. II, p. 181; MOREILLON, PAREIN-REYMOND, art. 10 N 8; PIQUEREZ, Traité de procédure pénale suisse, p. 182-183 ; Preuve-BOHNET, JEANNERET, p. 67; StPO-WOHLERS, art. 10 N 6.

l'accusé soit au bénéfice ou non d'une défense[292]. La présomption d'innocence prévue à l'art. 10 al. 1 et 2 CPP déploie ses effets tant qu'une question de fait est non-établie ou lorsqu'elle est douteuse. Ce n'est qu'à la fin de l'administration des preuves que le juge doit peser, de manière objective, les preuves à charge et à décharge[293]. Un jugement de culpabilité ne pouvant être rendu qu'après obtention de la certitude et hors de tout doute raisonnable, si objectivement les éléments constitutifs de l'infraction ne sont pas ou pas assez liés aux faits, si l'intention ou la négligence n'est pas affirmée ou si la culpabilité n'est pas, ou insuffisamment, démontrée, le juge applique l'adage *in dubio pro reo* qui tend à protéger le citoyen contre les risques d'une condamnation sans motivation, donc arbitraire[294].

290 Ainsi, le juge répressif ne peut se prévaloir d'un fait défavorable à l'auteur si, objectivement, des doutes sérieux et insurmontables subsistent[295]. Toutefois, il n'est nullement nécessaire que l'administration des preuves aboutisse à une certitude absolue et sans faille.

B. La liberté de la preuve et ses limites

1. Les principes

291 La liberté de la preuve (art. 139 al. 1 CPP) implique qu'il n'existe ni *numerus clausus* des moyens de preuves ni aucune hiérarchisation de la valeur probatoire. En outre, à moins que la loi en dispose autrement, tous les moyens probatoires pertinents sont exploitables.

292 En disposant l'applicabilité du système des preuves morales, le législateur désire laisser la porte ouverte à tout nouveau moyen de preuve pouvant potentiellement apparaître au gré des progrès scientifiques, de l'évolution des connaissances et de l'expérience[296]. Le juge et les parties peuvent donc administrer des moyens de preuves inédits, sous couvert de l'édiction d'une base légale – s'ils portent atteinte aux droits fondamentaux – et dans le strict respect du droit supérieur.

---

[292] VIAU, Preuve pénale, p. 105.

[293] ATF 120 Ia 31, 36-37 = JdT 1996 IV 79 = SJ 1994 541, 543-544; ATF 124 IV 86, 87-88 = JdT 1999 IV 136, 137-138; ATF 127 I 38, 40-41 = JdT 2004 IV 65, 67-68; ATF 137 IV 219, 227 = JdT 2012 IV 126, 133; ATF 138 V 74, 81-82; Message, Constitution, p. 188-189 ; Preuve-BOHNET, JEANNERET, p. 67.

[294] CORBOZ, p. 404; PERRIER DEPEURSINGE, art. 10, p. 28-29.

[295] Polizeiliche Ermittlung-VOSER, p. 31; SCHMID, Handbuch, p. 85-86; SCHMID, Praxiskommentar, art. 10 N 6 et 24.

[296] CR-CPP-BÉNÉDICT, TRECCANI, art. 139 N 10; MOREILLON, PAREIN-REYMOND, art. 139 N 2; SCHMID, Handbuch, p. 313.

293 Cependant, le principe de la liberté de la preuve n'est pas absolu; il souffre de certaines limitations.

294 En premier lieu, afin de respecter le principe de l'égalité des armes, seules les preuves versées au dossier (art. 77 let. g CPP) ou librement débattues (art. 107 CPP) à l'audience peuvent motiver la décision du juge.

295 En deuxième lieu, le moyen de preuve doit avoir une certaine assise et être pertinent[297]. L'art. 139 al. 1 CPP précise que les preuves licites sont utilisables sous conditions de l'état des connaissances scientifiques et de l'expérience quant à leur valeur et à leur véracité. A ce titre, la pertinence légale exige qu'une preuve soit licite – certains moyens illicites peuvent toutefois être apportés comme éléments probatoires (art. 141 al. 2 et 3 CPP) – et la pertinence logique demande l'existence d'un rapport entre le fait prouvé et le fait que l'on cherche objectivement à établir.

296 Ainsi, toute preuve logiquement pertinente et ayant une valeur probante suffisante est admissible à moins qu'elle fasse l'objet d'une règle d'exclusion en vertu de la loi. Cependant, le juge, bénéficiant de la libre appréciation des preuves, peut écarter une preuve même si elle est pertinente et légalement admissible[298].

2. Les méthodes interdites de preuves

297 Le Tribunal fédéral considère que toute personne est protégée contre "les atteintes qui tendraient, par un moyen quelconque, à restreindre ou à supprimer la faculté, qui lui est propre, d'apprécier une situation donnée et de se déterminer d'après cette appréciation"[299]. En concrétisation du respect de la dignité humaine, la recherche des preuves et leur administration doivent être réalisées dans le strict respect de loyauté et de la légalité des preuves[300]. Les moyens de preuves attentatoires, notamment aux droits de la défense, à l'intégrité psychique ou physique ainsi que les procédés contraires à la bonne foi sont proscrits[301].

---

[297] CR-CPP-BÉNÉDICT, TRECCANI, art. 139 N 9; MOREILLON, PAREIN-REYMOND, art. 139 N 5; RUCKSTUHL, DITTMANN, ARNOLD, p. 146; VIAU, Preuve pénale, p. 114-115.

[298] Infra Partie I, Chapitre 3, III, C, 1, n° 314-315.

[299] ATF 90 I 29, 36.

[300] CR-CPP-BENEDICT, TRECCANI, art. 139 N 6; JEANNERET, KÜHN, p. 181; MOREILLON, p. 143.

[301] BENEDICT, p. 44; CR-CPP-BENEDICT, TRECCANI, art. 139 N 11-14 et art. 140 N 1 ss; JEANNERET, KÜHN, p. 181-182; PERRIER DEPEURSINGE, art. 140, p. 191; PIQUEREZ, Traité de procédure pénale suisse, p. 336; RUCKSTUHL, DITTMANN, ARNOLD, p. 177-178.

298 Dans le strict respect de ce principe et de l'art. 140 al. 1 CPP qui le concrétise, les autorités policières ne peuvent pas, lors de l'interrogatoire du suspect, recourir à la force psychique ou physique. A l'instar de la torture, de la privation de sommeil ou de nourriture, les pressions morales, telles que la répétition anormale d'interrogatoire, sont prohibées dès lors qu'elles occasionnent un sentiment d'infériorité, d'humiliation, d'angoisse, de peur et brisent possiblement la résistance de l'accusé qui peut le mener à un faux aveu[302]. Il est également interdit – sous peine de toucher au noyau intangible de la liberté personnelle – d'annihiler la personnalité par l'utilisation de détecteurs de mensonges, de sérums de vérité, de narco-analyses ou d'alcooliser, voire d'hypnotiser la personne entendue[303]. Sont en outre exclus les ruses, stratagèmes ou promesses de nature à tromper l'individu l'amenant à faire des déclarations qu'il n'aurait pas faites dans des circonstances différentes[304]. En d'autres termes, toute méthode employant la contrainte, la force, les menaces, les promesses, la tromperie ou restreignant les capacités intellectuelles ou le libre arbitre sont interdits et les preuves administrées en violation de ces principes sont inexploitables (art. 140 al. 1 *cum* 141 al. 1 CPP).

299 Concernant, l'emploi d'un moyen de contrainte ou le recours à la force, il nous faut préciser que l'interdiction de l'art. 140 al. 1 CPP ne concerne que l'usage de la contrainte ou de la force contraire au droit pénal ou aux dispositions du Code de procédure pénale[305]. En effet, les mesures de contraintes sont des moyens adéquats qui peuvent sous certaines conditions être exécutées par les autorités pénales (art. 196 ss CPP).

3. L'exploitation des moyens de preuves obtenus illégalement

300 Chaque moyen de preuve doit obéir à des formalités qui lui sont propres, le non-respect des prescriptions légales viole le principe de la légalité dans la production des preuves. Néanmoins, le législateur a distingué trois catégories de règles en cas de preuves recueillies illégalement par l'autorité (art. 140 al. 1 à 3 CPP). Ajoutons une quatrième catégorie qui concerne les preuves recueillies illégalement par les particuliers.

---

[302] BENEDICT, p. 107-108; PIQUEREZ, Traité de procédure pénale suisse, p. 335-336; RIEDO, FIOLKA, NIGGLI, p. 167; SCHMID, Praxiskommentar, art. 140 N 1-2 et 6.

[303] ATF 109 Ia 273, 288-290 = JdT 1985 I 616, 619; ATF 131 I 272, 278; JEANNERET, KÜHN, p. 182; JOSITSCH, Strafprozessrechts, p. 88-89; Message, CPP, p. 1162; MOREILLON, PAREIN-REYMOND, art. 140 N 4; PERRIER DEPEURSINGE, art. 140, p. 191-192; RIEDO, FIOLKA, NIGGLI, p. 167; SCHMID, Praxiskommentar, art. 140 N 2.

[304] BÉNÉDICT, p. 107-108; MERLE, VITU, T. II, p. 198; Polizeiliche Ermittlung-ZUBER, p. 225-226; SCHMID, Praxiskommentar, art. 140 N 4.

[305] CR-CPP-BÉNÉDICT, TRECCANI, art. 140 N 10; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 119; MOREILLON, PAREIN-REYMOND, art. 140 N 6.

a. Les preuves absolument inexploitables

301 L'usage de moyens de preuves listés à l'art. 140 al. 1 CPP est formellement interdit. En effet, l'art. 141 al. 1 phr. 1 CPP rend – de manière absolue – inexploitable toute preuve obtenue en contrariété avec l'art. 140 al. 1 CPP[306].

302 Par ailleurs, l'art. 141 al. 1 phr. 2 CPP rappelle que des dispositions spécifiques du Code de procédure pénale dénoncent et interdisent l'exploitation de certains moyens de preuves. Tel est le cas notamment de l'enregistrement fait à l'insu d'une personne, si l'autorisation n'a pas été délivrée par le Tribunal des mesures de contrainte (art. 277 al. 1 et 2 CPP). Dans le cadre de notre sujet, nous pouvons encore citer l'interdiction de l'administration des documents séquestrés lorsque l'ayant-droit fait valoir son droit de refuser de témoigner (art. 248 al. 1 *cum* 264 al. 3), des enregistrements des communications qui concerne une personne tenue au secret professionnel et qui peut refuser de témoigner (art. 271 al. 3 *cum* 170-173)[307], des documents issus d'une découverte fortuite qui ne peuvent pas être utilisés (art. 278 al. 4 et 281 al. 4 CPP) et les informations ou informations fortuites recueillies par un agent infiltré dans la mesure où elle ne font pas l'objet ou n'aurait pas pu faire l'objet d'une autorisation d'investigation secrète (art. 289 al. 4 phr. 3 et 296 al. 1 CPP).

b. Les preuves relativement inexploitables

303 Lorsque la preuve est obtenue à la suite d'une violation d'une règle de validité, une pesée des intérêts doit être faite entre l'intérêt à poursuivre et la sauvegarde des droits de la personnalité de l'accusé (art. 141 al. 2 CPP). L'inexploitabilité de ces preuves est donc relative[308].

304 Ainsi, si une preuve obtenue illégalement est indispensable à l'élucidation d'une infraction grave, l'art. 141 al. 2 CPP permet son exploitation. Visant à rendre l'illégalisme de la preuve

---

306 DONATSCH, CAVEGN, RPS 2008, p. 164; PIETH, p. 163; Preuve-BOHNET, JEANNERET, p. 70; RIEDO, FIOLKA, NIGGLI, p. 169-170; RUCKSTUHL, DITTMANN, ARNOLD, p. 179; SCHMID, Praxiskommentar, art. 141 N 5.

307 ATF 141 IV 77, 82-87; ATF 138 IV 225, 228 = JdT 2014 I 24, 26.

308 PIETH, p. 163; Preuve-BOHNET, JEANNERET, p. 70; RIEDO, FIOLKA, NIGGLI, p. 171; RUCKSTUHL, DITTMANN, ARNOLD, p. 181; SCHMID, Praxiskommentar, art. 141 N 6; StPO-WOHLERS, art. 141 N 26.

sans conséquence, cette réglementation est fortement controversée en doctrine, puisqu'elle va à l'encontre de la bonne foi devant régir tout procès et viole l'interdiction de l'abus de droit[309].

305 A cette première problématique s'ajoute celle de la notion indéterminée d'"*infraction grave*". La large discrétion du juge peut mener à des décisions arbitraires – selon que le terme est interprété restrictivement ou largement –, voire inégalitaires.

c. La violation des règles d'ordre

306 En cas de violation d'une simple règle d'ordre, l'illégalisme ne rend pas inexploitable la preuve obtenue (art. 141 al. 3 CPP)[310].

d. L'effet en cascade de la règle d'exclusion

307 L'alinéa 4 de l'art. 141 CPP codifie une décision jurisprudentielle qui interdit d'exploiter une preuve dérivée si la première preuve obtenue illégalement était une condition *sine qua non*[311]. Cette condition doit permettre d'éviter les acquittements choquants alors même que la culpabilité est certaine[312].

308 Ainsi en droit suisse, l'effet induit est relatif. S'il paraît fortement vraisemblable que la preuve dérivée aurait pu dans tous les cas être recueillie, elle est exploitable. Dans le cas contraire, elle est exclue[313].

e. Le cas spécifique des preuves illégales recueillies par les particuliers

309 Dans le cas des preuves illégales recueillies par les particuliers (art. 12 et 13 *a contrario* CPP), les art. 139 ss CPP ne sont pas applicables faute d'être en présence d'un organe étatique[314].

---

309 BÉNÉDICT, p. 44; DONATSCH, CAVEGN, RPS 2008, p. 165; ROTH, p. 67.

310 EICKER, HUBER, p. 200; HAUSER, SCHWERI, HARTMANN, p. 282; JEANNERET, KÜHN, p. 185; PIQUEREZ, Traité de procédure pénale suisse, p. 460; Preuve-BOHNET, JEANNERET, p. 70; SCHMID, Strafprozessrecht, p. 260.

311 ATF 96 I 437, 440-441 = JdT 1972 I 217; ATF 99 V 12, 15; ATF 103 Ia 206, 217 = JdT 1979 IV 16, 22-23; ATF 130 I 126, 132; ATF 131 I 272, 274-275; ATF 133 IV 329, 332-333 = JdT 2009 IV 29, 32; ATF 134 IV 266, 288; ATF 138 IV 169, 171; Message, CPP, p. 1163; PERRIER DEPEURSINGE, art. 141, p. 194; Preuve-BOHNET, JEANNERET, p. 70.

312 SCHMID, Der Beweis, p. 83; SCHMID, Handbuch, p. 321.

313 CR-CPP-BÉNÉDICT, TRECCANI, art. 141 N 38; PIETH, p. 172.

Dès lors, le sort de ces preuves doit être tranché par les tribunaux au cas par cas[315], sauf, pour certains auteurs de doctrine, lorsque le Code de procédure pénale fixe l'exclusion indépendamment de la qualité de celui qui les a obtenues (notamment art. 140 CPP *cum* 141 al. 1 CPP)[316].

310 Hors cas visé par l'art. 140 *cum* 141 al. 1 CPP, plusieurs auteurs de doctrine et la jurisprudence admettent que le recueil d'une preuve par un particulier en violation d'une norme pénale implique les sanctions applicables aux autorités[317].

311 Néanmoins, plusieurs critères ont été proposés pour admettre ou exclure ce type de preuve. Le principe de *Beweisnotstand* – sorte d'état de nécessité dans le domaine de la preuve – admet une preuve illégale en violation d'une norme pénale, s'il y a urgence et que la proportionnalité ainsi que la subsidiarité sont respectées[318]. La doctrine et la jurisprudence ont considéré comme admissible une preuve illégale lorsqu'elle aurait pu être recueillie par l'autorité[319]. Enfin, la pesée des intérêts en présence est également un critère possible pour admettre ce type de preuve[320], étant précisé que l'avant-projet du Code de procédure pénale le prévoyait (art. 150 AP-CPP).

312 Concernant les règles de procédure, elles ne sont pas opposables aux particuliers[321]. Cependant, l'admissibilité sans réserve des preuves obtenues en violation du droit procédural par les particuliers n'est pas reconnue[322]. Par ailleurs, pour éviter qu'une règle de procédure destinée à protéger l'établissement de la vérité matérielle ou à garantir le principe de la bonne foi ne soit violé, la Cour cantonale de Zurich préconise de peser les intérêts en présence, ce

---

[314] CR-CPP-BÉNÉDICT, TRECCANI, art. 139-141 N 7; HAUSER, SCHWERI, HARTMANN, p. 286; JEANNERET, KÜHN, p. 187; SCHMID, Strafprozessrecht, p. 203.

[315] PAREIN, n° 30; SCHMID, Praxiskommentar, art. 141 N 3.

[316] CR-CPP-BÉNÉDICT, TRECCANI, art. 139-141 N 9-10.

[317] TF 1A.314/2000 du 5 mars 2001, c. 6; TF 1B_22/2012 du 11 mai 2012, c. 2.4.4; TF 6B_323/ 2013 du 3 juin 2013, c. 3.5; PERRIER DEPEURSINGE, art. 141, p. 193; PIQUEREZ, Traité de procédure pénale suisse, p. 46; SCHMID, Handbuch, p. 324-325; SCHMID, Strafprozessrecht, p. 202.

[318] BENEDICT, p. 231-233; JEANNERET, KÜHN, p. 188; PERRIER DEPEURSINGE, art. 141, p. 193; PIQUEREZ, Traité de procédure pénale suisse, p. 461; SCHMID, Handbuch, p. 324-325.

[319] TF 1A.314/2000 du 5 mars 2001, c. 6; TF 1B_22/2012 du 11 mai 2012, c. 2.4.4; TF 6B_323/ 2013 du 3 juin 2013, c. 3.5; TF 6B_983/2013 du 24 février 2014, c. 3.3.1; TF 6B_786/2015 du 8 février 2016, c. 1.2; GODENZI, p. 262 ss et 341 ss; HÄRING, p. 231-232.

[320] ATF 109 Ia 244, 246; TF 1B_22/2012 du 11 mai 2012, c. 1.3 et 2.4; OGer ZH, ZR 91/92 (1992/1993) 13-15, n° 8; GODENZI, p. 335 ss; SCHMID, Strafprozessrecht, p. 203.

[321] TF 6B_983/2013 du 24 février 2014, c. 3.3.1; TF 6B_786/2015 du 8 février 2016, c. 1.2; HAUSER, SCHWERI, HARTMANN, p. 286; Rapport explicatif relatif à l'avant-projet, p. 110; SCHMID, Strafprozessrecht, p. 203.

[322] TF 6B_744/2007 du 10 avril 2008, c. 2; TF 1B_22/2012 du 11 mai 2012, c. 2.4.4; TF 6B_323/ 2013 du 3 juin 2013, c. 3.5; TF 6B_983/2013 du 24 février 2014, c. 3.3.1; TF 6B_786/2015 du 8 février 2016, c. 1.2.

que réfute Niklaus Schmid[323]. Dès lors, hormis – vraisemblablement – pour les cas de violation prévue à l'art. 140 CPP, la question de l'admissibilité des preuves en violation d'une norme procédurale n'est pas tranchée.

C. La libre appréciation, l'intime conviction et le doute

313 L'exigence de l'établissement des faits découlant de la présomption d'innocence (10 al. 1 CPP) et de l'adage *in dubio pro reo* (10 al. 3 CPP) entrent en contact direct avec l'appréciation des preuves (art. 10 al. 2 CPP, corollaire de la liberté des preuves consacrée à l'art. 139 al. 1 CPP)[324].

1. La libre appréciation des preuves

314 Dans le système des preuves morales ou système de l'intime conviction, la liberté de la preuve impose aux législateurs de ne pas fixer par avance la valeur probatoire d'un moyen de preuve. Le juge est libre d'apprécier chacune des preuves, il le fait selon sa conscience et ses croyances, sans s'en remettre à ses sentiments personnels, et n'est lié ni par le genre ni par le nombre des preuves[325].

315 Ainsi, le juge peut exclure un moyen de preuve pertinent et légal s'il considère que la valeur probante n'est pas suffisante ou qu'il cause un préjudice disproportionné pour l'accusé[326]. De même, il peut se déclarer convaincu par un élément mineur, en défaveur de l'existence d'autres éléments contraires, notamment, il peut écarter l'aveu en faveur de simples déclarations[327]. Il n'est pas non plus lié par les conclusions de l'expert. Il peut également

[323] OGer ZH, ZR 91/92 (1992/1993) 13-15, n° 8; SCHMID, Handbuch, p. 324 ; ATF 109 Ia 244, 246; TF 1B_22/2012 du 11 mai 2012, c. 1.3 et 2.4; TF 1B_22/2012 du 11 mai 2012, c. 2.4.4; TF 6B_323/ 2013 du 3 juin 2013, c. 3.5.

[324] CR-CPP-BÉNÉDICT, TRECCANI, art. 139 N 2; CR-CPP-VERNIORY, art. 10 N 1; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 117; EICKER, HUBER, p. 37; PERRIER DEPEURSINGE, art. 10, p. 28-29; RIEDO, FIOLKA, NIGGLI, p. 36-37; RUCKSTUHL, DITTMANN, ARNOLD, p. 66-68; SCHMID, Praxiskommentar, art. 10 N 1; StPO-WOHLERS, art. 10 N 1.

[325] ATF 84 IV 171, 175 = JdT 1958 IV 155; ATF 103 IV 299, 300-301 = JdT 1978 I 476, 476-477; ATF 133 I 33, 36; ATF 135 V 53, 62; ATF 137 IV 219, 226 = JdT 2012 IV 126, 132; BACHELET, p. 67; CORNU Gérard, *Vocabulaire juridique*, 8ème éd., Paris 2007, p. 209; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 61 et 118; PERRIER DEPEURSINGE, art. 139, p. 190; RIEDO, FIOLKA, NIGGLI, p. 37; SCHMID, Handbuch, p. 82.

[326] CR-CPP-BÉNÉDICT, TRECCANI, art. 139 N 10; VIAU, Preuve pénale, p. 115.

[327] BOULOC, p. 124; CR-CPP-VERNIORY, art. 10 N 34.

fonder sa décision sur des moyens de preuves nouveaux ou inhabituels qui ont une valeur en vertu de la science, de la technique ou de l'expérience[328].

316 Cependant, le pouvoir discrétionnaire du juge n'est pas sans limite, dès lors que le droit procédural[329] et les droits de la défense doivent être respectés. Le principe d'immédiateté des débats, le droit d'être informé de ses droits et des faits à charge ainsi que le droit d'être entendu doivent permettre à l'accusé de préparer sa défense et de participer à la phase contradictoire. Ainsi, le juge n'appuie sa décision que sur des preuves ayant été produites à l'occasion des débats ou disponibles dans le dossier de procédure.

2. L'intime conviction et le doute

317 Le Code de procédure pénale invite les tribunaux à prendre une décision motivée en vertu de leur intime conviction (art. 10 al. 2 CPP *cum* 80 al. 2, 84 al. 1 et 5 CPP). Le juge est ainsi obligé de préciser les éléments de fait sur lesquels il fonde sa décision et doit faire preuve de cohérence dans son argumentation.

318 Propre au respect de la présomption d'innocence et à l'adage *in dubio pro reo*, le système de l'intime conviction emporte deux conséquences[330]. Lorsque le juge acquiert la certitude – exclusion de doutes irréductibles[331] – du déroulement des faits et de la faute de l'accusé, il rend une décision de culpabilité. Au contraire, dans l'hypothèse où le juge ne peut pas déterminer son intime conviction parce que des doutes insurmontables subsistent, il prononce l'acquittement. Toutefois, "*[u]ne simple et lointaine possibilité théorique que les faits réels puissent être différents ne suffit pas pour justifier un acquittement […].*"[332]. La violation de la présomption d'innocence n'est par conséquent invocable que dans l'hypothèse où "*après appréciation exempte d'arbitraire sur l'ensemble des preuves, le juge aurait dû éprouver des doutes sérieux et irréductibles sur la culpabilité de l'intéressé.*"[333].

---

328 SJ 1987 119, 124; RJJ 2004 269, 276.

329 Supra Partie I, Chapitre 3, III, B, n° 293 ss.

330 CR-CPP-VERNIORY, art. 10 N 46; JEANNERET, KÜHN, p. 73; JOSITSCH, Strafprozessrechts, p. 22; MOREILLON, PAREIN-REYMOND, art. 10 N 16-18; SCHMID, Praxiskommentar, art. 10 N 2 ss; StPO-WOHLERS, art. 10 N 11-14.

331 DONATSCH, SCHWARZENEGGER, WOHLERS, p. 60 et 118; Polizeiliche Ermittlung-VOSER, p. 31; SCHMID, Handbuch, p. 82.

332 ATF 137 IV 219, 226 = JdT 2012 IV 126, 132; RVJ 2000 288, 299-300.

333 ATF 120 Ia 31, 38-39 = JdT 1996 IV 79 = SJ 1994 541; ATF 124 IV 86, 89-91= JdT 1999 IV 136, 139-141; ATF 127 I 38, 40-41 = JdT 2004 IV 65, 67-68; ATF 135 V 53, 62.

319 Ainsi, l'adage *in dubio pro reo* doit être considéré davantage comme une règle de décision prescrivant au juge l'attitude à adopter en cas de doute et non une pure règle d'appréciation[334]. En tout état de cause, le juge doit, à l'aide des preuves administrées, transformer les soupçons en certitude pour permettre l'application du droit pénal[335]. Il ne fait donc plus de doute que la preuve est une prérogative essentielle et centrale à la procédure pénale.

IV. Les différents moyens de preuves

320 Théoriquement, il est impossible d'énumérer tous les moyens probatoires dès lors que la preuve pénale n'est pas soumise à un *numerus clausus*.

321 Cependant, environ sept catégories de preuves existent: l'audition du prévenu, les témoignages, l'audition des personnes appelées à donner des renseignements, les pièces à conviction, les observations faites sur les lieux de l'infraction, l'expertise qui peut être considérée comme une déclaration à titre de renseignement ou un indice, et les procès-verbaux. En outre, la doctrine classifie les preuves selon qu'elles sont indirectes, médiates ou par indices (A.), directes, matérielles ou immédiates (B.) ou hybrides (C.)[336].

A. Les constatations indirectes ou médiates

322 Les preuves indirectes ou médiates sont celles qui nécessitent un raisonnement logique et un examen critique approfondi pour pouvoir être appréciées à leur juste valeur.

323 Trois catégories de personnes peuvent fournir des preuves indirectes ou médiates: le prévenu entendu lors de l'interrogatoire (1.), les témoins interrogés au cours d'une audition (2.) et les personnes appelées à donner des renseignements (3.).

---

[334] Notamment: METTLER Christoph, "In dubio pro reo" – ein Grundsatz im Zweifel, in *PJA* 1999, p. 1107-1111, 1110; MÜLLER Jörg, *Der Grundsatz der freien Beweiswürdigung im Strafprozess (nach den Strafprozessordnungen des Bundes und des Kantons Zürich)*, Thèse de doctorat, Zurich 1992, p. 100; STRÄULI, La jurisprudence récente du Tribunal fédéral en matière de procédure pénale – Thèmes choisis, in *RPS* 114(1996), p. 60-75, 69.

[335] JOSITSCH, Strafprozessrechts, p. 2; SCHMID, Handbuch, p. 3 et 56-57.

[336] PIQUEREZ, Traité de procédure pénale suisse, p. 345; Polizeiliche Ermittlung-ZUBER, p. 220; RASSAT, p. 359; RIEDO, FIOLKA, NIGGLI, p. 164; RUCKSTUHL, DITTMANN, ARNOLD, p. 149.

1. L'interrogatoire du prévenu

324 Le prévenu peut faire des déclarations judiciaires à titre primaire devant une autorité judiciaire et des déclarations extrajudiciaires (aveux faits à un tiers, fuites, destructions d'objets essentiels à la détermination des faits, etc.).

325 Concernant les déclarations judiciaires, le Code de procédure pénale prévoit la possibilité à tous les stades de la procédure d'entendre le prévenu sur les faits qui lui sont reprochés (art. 157 à 161 CPP). Il s'agit "*d'entendre une personne à l'encontre de laquelle il existe des indices graves et concordants ou des charges suffisantes laissant supposer qu'elle a participé à la commission des faits reprochés […]*"[337].

326 Les déclarations du prévenu présentent juridiquement trois caractéristiques les distinguant de celles faites par les témoins[338]:

- la personne poursuivie n'est pas tenue de collaborer à l'administration de la justice. Elle n'est donc – en principe – pas tenue de comparaître et un refus de déférer à une citation du juge ne peut entraîner aucune sanction pénale.

- le prévenu n'est pas dans l'obligation de dire la vérité (art. 177 CPP). En effet, la loi reconnaît au prévenu le droit de se défendre par tous les moyens, au besoin par le mensonge[339].

- le prévenu n'est pas tenu de déposer, ni de répondre aux questions qui lui sont posées. Il a en effet le droit de garder le silence (art. 158 al. 1 let. b. CPP).

327 Durant l'audition, le prévenu peut donc avouer, faire des déclarations pouvant être exploitables comme preuve ou se taire.

328 A noter que, le juge étant libre d'apprécier les faits, l'aveu n'est plus une preuve absolue et la rétractation du prévenu peut ne pas être prise en considération[340]. En outre, en cas d'aveu, le juge doit vérifier que la confession ait été donnée librement, spontanément et de manière non-définitive[341].

---

[337] GUINCHARD, BUISSON, Procédure pénale, p. 452.

[338] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 144-145; PIQUEREZ, Traité de procédure pénale suisse, p. 348.

[339] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 145; MOREILLON, p. 143; RASSAT, p. 380.

[340] HAUSER, SCHWERI, HARTMANN, p. 245; JOSITSCH, Strafprozessrechts, p. 99; RSJ 96 (2000) p. 40; SCHMID, Praxiskommentar, art. 160 N 1; ST-YVES-ST-YVES, MEISSNER, p. 155. Supra Partie I, Chapitre 3, III, C, n° 313 ss.

[341] PIQUEREZ, Traité de procédure pénale suisse, p. 350; RASSAT, p. 381.

329 L'aveu revêt théoriquement la qualité de preuve classique. En pratique, l'historique de l'aveu en procédure pénale modifie légèrement la conception théorique, dès lors qu'il rassure l'enquêteur et le décideur. Ce ressentiment est dangereux, bon nombre d'aveux ne sont pas crédibles, voire inexacts; tel est le cas des aveux fournis par des personnes psychologiquement diminuées, jeunes ou mythomanes qui font preuve de vantardise ou encore des personnes affectivement liées à l'auteur[342].

330 Ainsi, l'aveu ne devrait jamais subordonner d'autres preuves, voire les rendre insignifiantes[343]. D'ailleurs, l'art. 160 CPP exige la continuation des investigations même en cas d'aveu, ceci dans le but de déceler la fausseté des aveux et d'obtenir d'autres preuves concordantes ou discordantes.

331 Quant aux simples déclarations, elles sont propres à apporter des éclaircissements sur le déroulement des faits ou sur la non-implication du prévenu. En revanche, les déclarations acquises par ruse, moyens de pression, violence, menace ou provocation doivent être écartées des débats (art. 140 al. 1 *cum* 141 al. 1 CPP)[344].

2. Le témoignage

332 Le témoignage ou preuve testimoniale est un récit utile fourni à la justice par une personne relatant ce qu'elle a constaté personnellement par la vue ou l'ouïe[345] – perception directe – ou ce qu'elle a appris ou entendu d'autres personnes – perception indirecte ou témoignage par ouï-dire[346].

333 Le contenu du témoignage n'est toutefois pas sans limite. Le rôle du témoin est d'exposer ce qu'il a vu, entendu ou appris; il ne doit en aucun cas faire part de son opinion personnelle ou de ses présuppositions sur les faits imputés au prévenu (art. 162 *a contrario* CPP). Dans le cas contraire, le juge doit mettre un terme à l'audition.

334 La qualité de témoin est reconnue à toute personne – autre que le prévenu (art. 157 ss CPP) et les personnes appelées à donner des renseignements (art. 178 ss CPP) – ayant des

---

342 BOULOC, p. 114; MERLE, VITU, T. II, p. 276.

343 RASSAT, p. 396; ST-YVES-ST-YVES, MEISSNER, p. 179-181.

344 JOSITSCH, Strafprozessrechts, p. 88-89; MOREILLON, p. 143; PERRIER DEPEURSINGE, art. 140, p. 191; SCHMID, Praxiskommentar, art. 140 N 2 ss et art. 141 N 5.

345 DONATSCH, SCHWARZENEGGER, WOHLERS, p. 149-150; JOSITSCH, Strafprozessrechts, p. 101; Polizeiliche Ermittlung-ZUBER, p. 254-255; SCHMID, Handbuch, p. 358-359; SCHMID, Praxiskommentar, art. 162 N 2.

346 ComEDH, Affaire *X c. République fédérale d'Allemagne*, arrêt du 7 juillet 1978, 8414/78, p. 234 et 236.

renseignements concernant l'acte délictuel ou l'auteur. Afin d'écarter les témoignages dont la crédibilité est d'emblée insuffisante, l'art. 163 al. 1 CPP exclut la capacité de témoigner aux personnes de moins de 15 ans et aux incapables de discernement.

335 En outre, le témoin a un statut particulier qui implique certains devoirs contrairement au prévenu:

- les témoins ont le devoir de témoigner (art. 176 CPP), sous réserve de l'application du droit de refuser (art. 168 ss CPP). Ainsi, ils sont astreints à collaborer avec la justice;
- en tant que devoir civique, le devoir de témoigner oblige le témoin à répondre à la citation à comparaître et à se présenter au procès, même s'il estime avoir le droit de refuser de témoigner[347];
- le témoin a l'obligation de déposer, soit de parler. Il ne peut pas se taire sans raison (art. 176 al. 1 et 177 al. 1 CPP);
- le témoin est exhorté à dire la vérité sous peine d'être poursuivi pour faux témoignage (art. 177 al. 1 CPP *cum* 307 CP)[348];
- le témoin doit en outre rester discret (art. 165 CPP) concernant son audition et celles auxquelles il a pris part[349].

336 Enfin, les témoins ont également des droits, notamment celui d'être indemnisé (art. 167 CPP), d'être protégé lorsqu'il existe un risque pour leur vie ou leur intégrité corporelle ou celle d'un de leurs proches (art. 149 CPP) ou de refuser de témoigner (art. 168 à 176 CPP).

337 La preuve testimoniale est la plus ancienne des preuves. Par son assise historique, elle est considérée comme l'une des preuves les plus importantes en procédure pénale. Le témoignage est, avec l'aveu, la preuve la plus utilisée, le témoin étant considéré comme "*les yeux et les oreilles de la justice*"[350].

338 Plusieurs raisons militent en faveur de cette preuve. La première tient à ce que l'audition des tiers soit moins suspecte que la déclaration du prévenu. La seconde se rapporte à la procédure orale et contradictoire adoptée par notre système juridique, dont le témoignage

---

[347] JdT 2002 III 27; CR-CPP-DONGOIS, art. 163 N 9-10; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 150; HAUSER, SCHWERI, HARTMANN,p. 270; RÉMY, p. 51; StPO-DONATSCH, art. 163 N 18.

[348] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 150; JOSITSCH, Strafprozessrechts, p. 102; SCHMID, Praxiskommentar, art. 177 N 2.

[349] CR-CPP-DONGOIS, art. 165 N 4; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 150; SCHMID, Praxiskommentar, art. 165 N 1 ss; Polizeiliche Ermittlung-ZUBER, p. 256.

[350] BENTHAM, Vol. I, p. 191-192; ST-YVES-GEISELMAN, FISHER, p. 31.

offre un respect total. La troisième est la possibilité d'étendre les déclarations des témoins à l'aide de questions posées par la défense, l'accusation ou par le juge.

339 Néanmoins, le témoignage reste incertain, fragile et approximatif[351]. Les dires du témoin peuvent être entachés de mensonges – faussetés de l'audition consciente dues à la haine ou à la sympathie – ou d'erreurs – faussetés inconscientes – puisque la mémoire n'est pas infaillible.

340 A l'image des autres preuves, la preuve testimoniale n'a pas la qualité de reine des preuves. Le raisonnement critique, lors de l'appréciation d'une déclaration par le juge, doit tenir compte tant de la valeur morale – moralité générale, capacité intellectuelle, dispositions affectives – que des facultés psychologiques du déposant et de la valeur de la déposition elle-même en décelant les mensonges ou les réticences[352].

3. Les personnes appelées à donner des renseignements

341 Les "*personnes appelées à donner des renseignements*" forment une catégorie particulière et subsidiaire d'informateurs entendus par la justice répressive[353]. Il s'agit d'un statut intermédiaire sis entre celui du prévenu et celui du témoin[354].

342 La création de cette catégorie est nécessaire pour rechercher la vérité matérielle qui impose d'entendre toutes personnes susceptibles de fournir des informations et pour prendre en considération les situations où il n'est pas exigible d'attendre d'une personne qu'elle dépose conformément à la vérité, notamment du fait de son jeune âge (art. 178 let. b CPP), de ses facultés mentales ou psychiques restreintes (art. 178 let. c CPP) ou de sa position dans la procédure (art. 178 let. d à g CPP). C'est pourquoi, la personne appelées à donner des renseignements doit comparaître, mais n'est pas tenue par l'obligation de témoigner (art. 163 et 176 CPP), et ne risque pas d'être poursuivie pour faux témoignage.

343 Pour le surplus, les bases légales relatives à l'interrogatoire du prévenu sont applicables par analogie.

---

[351] PERRIER DEPEURSINGE, art. 162, p. 215; Polizeiliche Ermittlung-ZUBER, p. 255; RASSAT, p. 416; RUCKSTUHL, DITTMANN, ARNOLD, p.163-170; ST-YVES-HOPE, SAUER, p. 103 et 121-122.

[352] FRANCHIMONT, JACOBS, MASSET, p. 1073-1074.

[353] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-ILL, p. 169; SCHMID, Praxiskommentar, art. 178 N 1-2.

[354] JOSITSCH, Strafprozessrechts, p. 106; PERRIER, VUILLE, p. 125; Polizeiliche Ermittlung-ZUBER, p. 265; RUCKSTUHL, DITTMANN, ARNOLD, p.171.

344 Relevons encore que le lésé qui se constitue partie plaignante (art. 118 CPP) est entendu à titre de renseignement (art. 178 let. a CPP) avec un régime particulier. Il ne peut pas être condamné pour faux témoignage[355], mais il est astreint à déposer devant les tribunaux (art. 180 al. 2 CPP). Dans ce cas de figure, les dispositions concernant l'audition des témoins s'appliquent par analogie exception faite de l'art. 176 CPP.

345 Les déclarations des personnes appelées à donner des renseignements ont une valeur probante similaire au témoignage. Juridiquement, le juge est en droit de préférer une déclaration faite à titre de renseignement plutôt qu'un témoignage[356].

346 Cependant, il est contestable qu'une déposition faite par une personne appelée à donner des renseignements soit aussi fiable qu'un témoignage pour deux raisons. Premièrement, les personnes appelées à renseigner sont soit parties intéressées quant à l'issue du procès – c'est le cas du lésé qui s'est constitué partie plaignante (art. 178 let. a CPP), du co-prévenu visé sous let. d et e de l'art. 178 CPP –, soit des auteurs, instigateurs ou complices des faits délictueux qui n'ont pas la qualité de prévenu, soit des personnes ne pouvant pas être témoin à défaut d'avoir une crédibilité suffisante. Deuxièmement, ces personnes n'ont pas la crainte de la sanction pénale en cas de faux témoignage. Pouvant mentir en toute impunité, le risque de déclaration infidèle à la réalité est augmenté.

347 Par conséquent, il serait préférable que le juge évalue la crédibilité du ou des renseignements fournis par les personnes visées à l'art. 178 CPP pour écarter, par exemple, un témoignage.

B. Les constatations directes ou immédiates

348 Les constatations directes ou immédiates sont des preuves réelles ou purement matérielles, le juge acquiert personnellement et immédiatement la connaissance du fait ou d'une chose en lien avec l'affaire à juger.

349 Le Code de procédure pénale scinde les preuves déduites des choses en deux groupes distincts: les éléments pouvant être directement versés au dossier (1.) et les éléments qui, en raison de leur nature, ne peuvent être intégrés qu'indirectement au dossier d'enquête (2.)[357].

---

[355] CR-CPP-PERRIER, art. 180 N 19; PIETH, p. 180-181.

[356] ATF 117 Ia 401, 405 = JdT 1993 IV 192; PIQUEREZ, Traité de procédure pénale suisse, p. 359.

[357] CR-CPP-PONCET CARNICÉ, art. 192 N 4; PIQUEREZ, Traité de procédure pénale suisse, p. 519; SCHMID, Handbuch, p. 397.

1. Les pièces à conviction

350 Les pièces à conviction (art. 192 CPP) font parties des preuves émanant souvent des choses mobilières ou des traces[358].

351 Les pièces à conviction regroupent divers moyens de preuves recueillis pouvant être directement versés au dossier ou faire l'objet d'une annexe[359]. Leur forme peut varier à l'infini: éléments propres au corps du délit (lettre comprenant une menace ou une atteinte à l'honneur, fausse monnaie ou faux document, etc.), objets se rapportant à la commission de l'infraction (arme du crime), objets relatifs à l'exécution d'un acte délictueux (argent blanchi, chose mobilière endommagée ou volée), voire tout objet sans rapport direct avec l'infraction, mais de nature à être utilisé au cours du procès pénal (objet personnel du suspect retrouvé sur les lieux d'une infraction), traces (cheveu, fibre textile, empreinte digitale ou plantaire, sang ou empreinte ADN), ou tout autre objet de preuve relevant particulièrement des écrits[360] ou d'enregistrements (titre, lettre, carnet d'adresses, contrat, listing d'ordinateurs, disquette ou autre support magnétique)[361].

352 Le Conseil fédéral considère les indices comme des pièces à conviction[362]. Sans nul doute, un indice ne nécessitant pas de connaissances spécifiques pour être interprété peut être considéré comme une preuve directe. Il en va différemment lorsque le recours à un spécialiste est inévitable pour le faire "parler".

353 La preuve directe comprend tout élément qui permet à l'autorité répressive d'acquérir personnellement et immédiatement la connaissance d'un fait, dans l'hypothèse où un indice nécessite l'appel à un expert, cet élément probatoire est lié à une présomption de l'homme qui altère la qualité de preuve directe. C'est pourquoi nous sommes d'avis qu'il faut considérer ce type d'indice comme une preuve hybride[363].

354 Selon le principe de la libre appréciation des preuves, les pièces à conviction n'ont, juridiquement, pas une valeur probante supérieure aux autres moyens de preuves. Ainsi,

---

[358] JEANNERET, KÜHN, p. 251; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 182; SCHMID, Praxiskommentar, art. 192-195 N 1-2;.

[359] ; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 182; JEANNERET, KÜHN, p. 251; KAUFMANN, p. 179.

[360] A ce sujet: HAUSER, SCHWERI, HARTMANN, p. 276 et 319; PERRIER DEPEURSINGE, art. 192, p. 240; SCHMID, Handbuch, p. 398; SCHMID, Praxiskommentar, art. 192 N 3.

[361] KAUFMANN, p. 179-180; SCHMID, Handbuch, p. 397; SCHMID, Praxiskommentar, art. 192-195 N 1.

[362] Message, CPP, p. 1194.

[363] Infra Partie I, Chapitre 3, IV, C, 1, n° 364-366.

tout objet ou trace original peut être versé au dossier. En outre, l'art. 192 al. 2 CPP prévoit que les titres ou autres documents peuvent être de simples copies ce qui peut influer sur leur valeur puisqu'ils ne sont pas authentifiés[364].

355 En pratique, les pièces à conviction par leur nature matérielle sont appréciées de la justice répressive qui leur porte un grand intérêt. En effet, contrairement aux êtres humains, un objet, une trace ou un écrit dépourvu de parole n'a pas la possibilité de mentir. Par sa nature, la pièce à conviction établit un fait scientifiquement et/ou objectivement. La manipulation de la preuve matérielle est, dans l'esprit d'une majorité de la population, moins évidente rendant les pièces à conviction plus crédibles, puisque plus fidèles à la réalité[365].

2. Les observations du lieu de l'infraction

356 A tous les stades de la procédure, le ministère public, le tribunal et, dans des certains cas, comme les accidents de la route, la police se rendent sur les lieux de l'infraction pour y faire les constatations nécessaires à la découverte de la vérité matérielle. Communément appelé le transport sur place, la preuve par l'inspection comprend au sens large la preuve matérielle et les constatations *de visu*.

357 En édictant l'art. 193 CPP, le législateur a voulu traiter la preuve par l'inspection dans son sens étroit, c'est-à-dire la preuve s'attachant aux objets importants en termes probatoires ne pouvant pas être versés directement au dossier en raison de leur nature[366].

358 Lors du transport sur place, l'autorité procède à toutes les opérations nécessaires à la manifestation de la vérité: visualisation des lieux, analyse de la situation, de la configuration, de la luminosité, etc.[367]. L'inspection permet d'effectuer personnellement – par ses propres sens – toutes les constatations utiles à l'élucidation des faits, notamment pour recueillir des preuves ou indices, visiter, décrire et reconstituer les événements, ainsi que perquisitionner, saisir, voire photographier les lieux et objets utiles[368]. Chacune des opérations effectuées fait l'objet d'un procès-verbal circonstancié ou éventuellement d'un enregistrement sonore, de

---

[364] HAUSER, SCHWERI, HARTMANN, p. 319; SCHMID, Praxiskommentar, art. 192 N 4.

[365] Infra Partie II, Chapitre 2 et Chapitre 3, n° 610 ss, 906 ss, 1235 ss, 1563 ss, 1780 ss, 2095 ss et 2227 ss.

[366] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 169; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 183; KAUFMANN, p. 180; PIETH, p. 185; Rapport explicatif relatif à l'avant-projet, p. 144; SCHMID, Praxiskommentar, art. 192-195 N 3.

[367] OBERHOLZER, Strafprozessrechts, p. 303; PIQUEREZ, Traité de procédure pénale suisse, p. 395; SCHMID, Strafprozessrecht, p. 237.

[368] ATF 121 V 150, 153; HAUSER, SCHWERI, HARTMANN, p. 315; SCHMID, Handbuch, p. 399.

plans, de dessins et des descriptions des éléments visualisés[369]. Le transport peut aussi concerner la victime – conclusion prise suite à l'analyse des blessures, (art. 252 CPP) ou enquête en cas de mort suspecte (art. 253 CPP) – soumise à un examen corporel ou à une autopsie ordonnée par le juge. L'inspection peut également revêtir la qualité d'une reconstitution ou d'une confrontation entre les diverses personnes impliquées dans la procédure[370].

359 Corrélativement aux pièces à conviction, l'observation des lieux de l'infraction n'a pas de valeur probante supérieure à une autre preuve. Toutefois, en tant que preuve directe ou matérielle, l'inspection est – d'après l'avis des magistrats – l'un des moyens de preuves et de renseignement fiable et véridique. La supériorité pratique découle du fait qu'en tant que preuve matérielle, elle est objective et le juge peut l'appréhender de façon immédiate, personnelle et sensorielle sans influence extérieure même inconsciente. Il s'agit d'une preuve d'évidence à l'instar des preuves sous la forme de pièces à conviction.

C. Les constatations hybrides

360 Lorsque le juge aurait pu observer personnellement et déduire seul la force probante d'une preuve, mais, par manque de connaissances spécifiques ou par économie de procédure, un intermédiaire – expert ou rédacteur d'un procès-verbal – est appelé à participer à l'interprétation ou à la récolte des preuves, la preuve matérielle n'est plus directe. Ces preuves fournies en partie par les choses et en partie par les personnes se situent entre les constatations matérielles des faits et les constatations médiates.

361 Nous pouvons regrouper dans la catégorie des constatations hybrides les indices devant être interprétés (1.) et les procès-verbaux relatifs à la phase d'enquête ou d'instruction ainsi qu'à la recherche de preuve (2.).

1. L'expertise

362 Au vu de l'importance de l'expertise dans le cadre de notre travail, ce mode probatoire fait l'objet d'un chapitre distinct[371]. Cela étant, la présente partie énumérant les divers moyens de

[369] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 183.

[370] HAUSER, SCHWERI, HARTMANN, p. 18; OBERHOLZER, Strafprozessrechts, p. 304; SCHMID, Handbuch, p. 399; SCHMID, Praxiskommentar, art. 192-195 N 3.

[371] Infra Partie II, Chapitre 1, n° 385 ss.

preuves, nous nous devons d'expliquer, dans la présente partie, en quoi ce moyen de preuve est une constations hybride. Pour le surplus, nous renvoyons le lecteur à la partie supra précitée.

363 L'indice se définit comme un fait, un élément ou une circonstance se rapportant à l'infraction et permettant de déterminer l'existence ou les modalités de la perpétration d'un acte délictuel ainsi qu'éventuellement l'identité d'un suspect ou d'un prévenu. Il peut s'agir d'indices matériels tirés de la conduite ou de l'attitude d'une partie ou d'un témoin, d'objets et de traces recueillis sur les lieux et/ou sur les personnes, ou d'indices comportementaux.

364 Contrairement aux indices matériels, les indices comportementaux peuvent être constatés et interprétés par le seul raisonnement du juge, notamment en vérifiant un alibi. L'indice matériel requiert généralement des connaissances spécifiques approfondies pour être interprété[372].

365 Lors de l'analyse d'un indice matériel, le recours à l'expert peut être considéré comme un passage obligatoire pour comprendre et établir un fait[373]. L'expert joue le rôle d'intermédiaire entre une preuve normalement directe – pièce à conviction, trace ou objet découvert – et ce qu'elle démontre en finalité. Par exemple, trouver une trace de sang n'est en soi pas une preuve, il faut encore l'analyser et la traiter pour déterminer si elle identifie un éventuel suspect.

366 Ainsi, lorsqu'une preuve matérielle nécessite le recours à un expert pour la faire "parler", il ne s'agit plus d'une preuve directe, mais d'une preuve hybride[374]. Il nous faut spécifier que l'appel à un spécialiste ne rend pas la preuve indirecte. En effet, il serait erroné de considérer la valeur de la parole d'un expert indépendant dont la nomination est conditionnée au respect de dispositions légales strictes[375] à celle du prévenu, d'un témoin ou d'une personne appelées à donner des renseignements pouvant avoir un parti pris dans l'affaire.

367 Depuis quelques années, cette preuve par indice matériel a connu un essor considérable en matière pénale, ce qui s'explique par la variété infinie des indices et des progrès des

---

[372] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 163; PIETH, p. 183-184; PIQUEREZ, Traité de procédure pénale suisse, p. 380; RASSAT, p. 417-418; VIAU, Preuve pénale, p. 126.

[373] BOULOC, p. 113; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 163; JOSITSCH, Strafprozessrechts, p. 108; PIETH, p. 183-184; SCHMID, Handbuch, p. 384; SCHMID, Praxiskommentar, art. 182 N 1.

[374] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 174; Polizeiliche Ermittlung-ZUBER, p. 276.

[375] Infra Partie II, Chapitre 1, n° 408 ss et 424 ss.

techniques d'interprétation[376]. Conséquemment, l'expertise s'est immiscée en procédure pénale pour confirmer scientifiquement les dires d'une personne ou identifier un individu[377].

368 La conclusion du rapport d'expertise n'a juridiquement pas de valeur probatoire, il s'agit d'un simple avis technique soumis à la libre appréciation du juge[378]. Cette liberté offerte au magistrat lui permet de déroger à la conclusion de l'expertise, si, d'un point de vue juridique, il peut justifier sa décision[379]. Naturellement, nous pourrions nous interroger s'il existe réellement une autonomie entre les conclusions de l'expert et le choix du juge. Nous laissons la question ouverte à ce stade de l'analyse, l'expertise et les nouvelles technologies étant au cœur de notre deuxième partie et de notre conclusion.

2. Les procès-verbaux

369 En procédure pénale, tous les actes de procédure doivent être consignés dans un procès-verbal comme l'impose l'obligation de documenter faisant partie intégrante de la bonne tenue des dossiers (art. 100 CPP)[380] et du droit de consultation (art. 107 CPP), extensivement du droit d'être entendu[381].

370 Aux articles 76 à 79, le Code de procédure pénale traite des principes généraux relatifs à l'obligation de documenter, plus précisément des exigences concernant la tenue des procès-verbaux. Tous les actes de procédure pénale doivent être consignés de manière appropriée et être versés au dossier. Le procès-verbal retrace normalement dans l'ordre chronologique tous les faits accomplis s'étendant de la procédure d'enquête de police jusqu'à l'entrée en force du jugement permettant un contrôle *a posteriori* des actes de procédure[382].

371 De manière générale, le préposé au procès-verbal – membre de la police judiciaire, ministère public, magistrat ou greffier – relate par écrit les infractions constatées et les résultats des

[376] FRANCHIMONT, JACOBS, MASSET, p. 786.

[377] Infra Partie II, Chapitre 1, I, C, n° 418 ss.

[378] JOSITSCH, Strafprozessrechts, p. 111; PERRIER DEPEURSINGE, art. 189, p. 238; PIETH, p. 188; SCHMID, Handbuch, p. 395.

[379] Infra Partie II, Chapitre 1, III, B, 2, n° 494-495; Infra Partie II, Chapitre 1, III, C, 1, n° 498-502 et 504.

[380] PERRIER DEPEURSINGE, art. 100, p. 124; Polizeiliche Ermittlung-RHYNER, p. 108; SCHMID, Praxiskommentar, art-76-79 N 3.

[381] Polizeiliche Ermittlung-RHYNER, p. 108; SCHMID, Praxiskommentar, art. 76-79 N 3 et art. 78 N 10.

[382] CR-CPP-CHAPUIS, art. 101 N 2; Message, CPP, p. 1133; PERRIER DEPEURSINGE, art. 101, p. 125; SCHMID, Praxiskommentar, art. 76 N 2.

opérations effectuées avec leurs déroulements[383]. Les procès-verbaux sont des actes authentiques témoignant des observations visuelles ou auditives dont le fonctionnaire a pris personnellement connaissance. Ces écrits peuvent être utilisés – complètement ou en partie – pour établir un fait nécessaire à la détermination de l'infraction ou de la culpabilité du prévenu.

372 Le procès-verbal de procédure (art. 77 CPP) sert à documenter les diverses phases de procédure. Il s'agit des procès-verbaux de confrontations (art. 146 al. 2 CPP), d'inspections ou de constatations (art. 192 ss CPP), de perquisitions (art. 244 ss CPP), de séquestres (art. 264 ss CPP), de surveillances de la correspondance par poste et télécommunication (art. 269 ss CPP), d'observations (art. 282 ss CPP), d'investigations secrètes (art. 285a ss CPP) et de recherches secrètes (art. 298a ss CPP)[384]. Ces procès-verbaux consignent le plus fidèlement possible notamment la nature de l'acte, le lieu, le contenant, les objets découverts lors de la perquisition, de la saisie, l'identité des personnes présentes, les conclusions des parties, les observations, etc.[385].

373 Concernant les procès-verbaux suite à une inspection, dans le cadre des constatations hybrides, il ne s'agit pas de retenir les procès-verbaux faisant état d'observations perçues par le juge, mais uniquement des procès-verbaux rédigés suite au transport sur les lieux de l'infraction sans que le juge soit présent et donc sans qu'il ne puisse personnellement constater les éléments probatoires.

374 Le procès-verbal des auditions (art. 78 CPP) regroupe les informations sur le déroulement et le contenu des interrogatoires et témoignages[386]. La rédaction de ces procès-verbaux doit être faite chronologiquement et directement après la déposition orale, soit séance tenante (art. 78 al. 1 CPP). Suivant la pratique adoptée par les cantons, le Code de procédure pénale suisse n'exige pas une retranscription textuelle des questions posées et des réponses apportées[387]. La suppression de la question et la consignation unique de la réponse ou le résumé de plusieurs réponses est acceptable. Ce procédé peut poser problème quant à la fiabilité de la retranscription, il n'est jamais évident de synthétiser un dire sans lui ôter – du moins en partie – sa substance. C'est pourquoi, l'art. 78 al. 3 CPP précise que les questions et réponses

---

[383] CR-CPP-CHAPUIS, art. 101 N 1; PIQUEREZ, Traité de procédure pénale suisse, p. 565.

[384] Polizeiliche Ermittlung-RHYNER, p. 124-127;.

[385] PIQUEREZ, Traité de procédure pénale suisse, p. 160-161 et 565; Polizeiliche Ermittlung-RHYNER, p. 124-125; SCHMID, Praxiskommentar, art. 77 N 1 ss.

[386] CR-CPP-BOMIO, art. 78 N 1; PERRIER DEPEURSINGE, art. 78, p. 98; Polizeiliche Ermittlung-RHYNER, p. 120; SCHMID, Praxiskommentar, art. 78 N 2.

[387] Message, CPP, p. 1134; PERRIER DEPEURSINGE, art. 78, p. 98; SCHMID, Praxiskommentar, art. 78 N 5.

déterminantes pour l'avenir de la procédure doivent être consignées textuellement. Il est opportun de faire preuve de retenue quant à savoir si une question ou une réponse peut être synthétisée, puisque cette problématique intervient préalablement à la prise de connaissance par le juge des déclarations. Il contreviendrait à la libre appréciation des preuves d'écarter trop aisément un dire qui finalement serait essentiel à l'établissement d'un fait lié à l'affaire pénale.

375 Concernant la valeur probante, les procès-verbaux d'audition, de procédure ou de constatations sont des actes authentiques rédigés de bonne foi et relatant avec exactitude le déroulement des diverses phases procédurales. La plupart des dispositions relatives à la tenue des procès-verbaux – exception faite de l'art. 78 al. 2 et 3 qui sont des règles d'ordre dont l'irrespect peut seulement occasionner une diminution de la valeur probante – sont impératives et ne souffrent d'aucune dérogation. Le non-respect des conditions légales occasionne l'inexploitation des documents.

376 Conformément au principe de la liberté de la preuve, lorsque les prescriptions impératives sont respectées, toutes les formes de procès-verbaux ont la même force probante égale à celle valant pour les autres moyens de preuves[388]. En pratique, généralement, les procès-verbaux des audiences n'ont pas de force probante particulière, ils sont considérés comme de simples renseignements. Les autres procès-verbaux peuvent – au contraire – être administrés comme preuve – appelée preuve de la justesse par document – soit du respect des conditions de procédure, soit d'un fait ou de la culpabilité du prévenu. Sans hiérarchiser et reconnaître une force probatoire prépondérante à l'une ou à l'autre des formes de procès-verbaux, des préjugés existent différenciant le procès-verbal d'audition du procès-verbal de procédure.

377 Concernant spécifiquement la valeur probatoire des procès-verbaux d'audition, il existe un risque plus ou moins important que des dépositions soient faussées ou que des éléments décisifs ne soient pas consignés textuellement. La prise en compte de ce risque restreint d'office la valeur probatoire des procès-verbaux d'audition. Dans la mesure du possible, si le juge peut entendre l'auteur de la déposition, le procès-verbal d'audition doit être considéré comme un simple renseignement complémentaire.

378 Concernant les procès-verbaux rédigés suite à une inspection sans la présence du juge, il semblerait judicieux d'exiger du fonctionnaire de certifier avoir accompli personnellement les constations retranscrites, de ne rédiger que les observations matérielles sans opinion propre, d'effectuer les observations dans l'exercice de ses fonctions et de remplir les conditions de

[388] PIQUEREZ, Traité de procédure pénale suisse, p. 565.

forme et de fond. Sous le couvert du respect de ces quatre conditions, il semblerait acceptable de reconnaître à ces procès-verbaux la même force probante que les constations directes effectuées par le juge lui-même.

379 Bien que des différences de force probante entre les divers types de procès-verbaux existent, elles sont minimes et le juge reste libre de les apprécier.

DEUXIÈME PARTIE: LES NOUVELLES TECHNOLOGIES COMME MOYEN DE PREUVE

380 Toute procédure pénale est centrée sur la détermination de la vérité matérielle des faits à juger. Il en découle une volonté d'administrer des preuves à charge et à décharge assorties d'une crédibilité patente. Les techniques et les sciences, par leur objectivité, répondent positivement à ce désir.

381 Pour interpréter correctement les circonstances de fait liées à un domaine technique ou scientifique, des connaissances spécifiques dudit domaine sont nécessaires. Le juge, désireux d'exploiter une preuve scientifique ou technique ou de délimiter ce qu'elle prouve selon l'état de fait, doit faire intervenir quasiment inévitablement un expert afin de faire "parler" les indices. L'intégration des domaines scientifiques et techniques en procédure pénale oblige régulièrement la justice à recourir à l'expertise pour comprendre une preuve et établir sa fiabilité.

382 Les domaines scientifiques ou techniques sont variés. Il peut s'agir des recherches à la suite d'analyses de traces, on pensera à l'utilisation des empreintes digitales ou de l'ADN; des méthodes liées à la surveillance ou à la localisation qui ont connu une évolution au niveau des moyens employés (écoute téléphonique, vidéosurveillance, GPS, téléphone mobile ou messagerie électronique); ou des possibilités données par l'informatique pour rechercher des auteurs d'infraction, pour stocker et pour exploiter des informations à l'aide des bases de données.

383 Le progrès technique permet de mieux collecter, examiner, voire conserver des traces ou des indices découverts sur les lieux d'une infraction. Ces modes probatoires ne sont plus relégués à un simple usage occasionnel. Ils sont devenus essentiels à l'administration de la justice pour resserrer l'étau de la condamnation sur les auteurs d'infraction[389] et établir le déroulement des faits délictueux. Néanmoins, les possibilités offertes par ces nouvelles technologies dans le cadre procédural ne sont pas exemptes de défauts, notamment quant à la protection des droits de la personnalité.

384 Ces constats axent la direction de notre travail. L'étude des domaines traités s'intéresse à l'examen de l'objet et du contexte pratique des nouvelles technologies et au contexte juridique dans le dessein d'établir la force, la faiblesse et les incertitudes des moyens de preuves

[389] CORNU, p. 237.

technologiques ou scientifiques, de dévoiler les conflits que leurs usages engendrent sur le plan des droits fondamentaux et procéduraux, et d'établir la réalité sur leur valeur probante. L'administration des nouvelles technologies comme moyen de preuve engendrant le recours quasi systématique à un expert, une première partie de notre travail est dévolue spécifiquement aux conditions générales – procédurales et professionnelles – et à la problématique de l'expertise en procédure pénale (Chapitre 1). Concernant les chapitres suivants sur les nouvelles technologies, nous avons pris position d'analyser celles qui ont eu le temps d'être accueillies, adoptées, voire transformées par les décisions jurisprudentielles, l'avis de la doctrine ou la législation, considérées comme tangibles pour découvrir totalement ou partiellement la vérité matérielle et qui ne sont pas prohibées par le Code de procédure pénale. Les techniques trop récentes font l'objet de la perspective d'avenir. Elles ne sont pas détaillées dans le présent travail. Ainsi, la recherche est menée sur deux types de preuve: les preuves fondées sur les sciences (Chapitre 2) et les preuves fondées sur les techniques (Chapitre 3). Les sciences se définissant comme l'ensemble des connaissances qu'on acquiert par l'expérience, l'observation et par des déductions logiques, nous intégrons à ce domaine la dactyloscopie et la génétique. Dans le cadre de l'étude des techniques, nous étudions les applications ou concrétisations matérielles de certaines sciences, notamment informatisées, comme les télécommunications, la vidéosurveillance, le GPS et l'informatique.

CHAPITRE 1: L'EXPERTISE

I. Les généralités

A. La définition et la notion

385 L'expert joue un rôle central en procédure. Il est un acteur indispensable dans la recherche de la vérité. Qu'il s'agisse d'une demande du ministère public ou des tribunaux (art. 182 ss CPP), l'appel à un ou plusieurs spécialistes chargés d'effectuer une expertise judiciaire est licite pour élucider une problématique liée au manque de connaissances des juristes. Le recours à un expert est une des caractéristiques principales de la phase dite scientifique du système de preuve morale[390].

386 Un expert peut intervenir dans de nombreux domaines, notamment lors de la réalisation d'un projet législatif, comme contrôleur pour déterminer l'état de fonctionnement d'un véhicule, pour appréhender la capacité de discernement et/ou la responsabilité d'un individu, etc. Nous ne traitons toutefois que de l'expert au sein de la procédure pénale qui peut intervenir dans le domaine médical, biologique, toxicologique, des sciences forensiques ou informatiques.

387 En procédure, l'expertise est un procédé permettant de découvrir et d'utiliser certains indices ou certaines preuves grâce aux connaissances scientifiques ou techniques particulières[391]. Cette définition englobe l'expertise judiciaire correspondant à l'exécution d'un mandat du juge ou du ministère public et l'expertise privée lorsque la mission est accomplie sous la direction d'une partie au procès[392].

388 Dans le cadre de l'administration des preuves en procédure pénale, il s'agit de distinguer ces deux types d'expertise et de définir plus précisément l'expertise judiciaire.

---

390 Supra Partie I, Chapitre 1, II, A, 3, b, n° 66-67.

391 BÜHLER, p. 567; DONATSCH, CAVEGN, RPS 2008, p. 171; MERLE, VITU, T. II, p. 258; RUCKSTUHL, DITTMANN, ARNOLD, p. 172-173.

392 CPP-Commentario-GALLIANI, MARCELLINI, art. 182-191 N 4; CR-CPP-VUILLE, art. 182 N 18 ss; DONATSCH, Jusletter, n° 8; PERRIER DEPEURSINGE, art. 182, p. 230-231; PIQUEREZ, Traité de procédure pénale suisse, p. 380-381; RUCKSTUHL, DITTMANN, ARNOLD, p. 173.

389 Etant une simple allégation d'une partie[393], l'expertise privée est considérée comme un moyen de preuve irrégulier qui n'est pas expressément prévu par le Code de procédure pénale. L'expertise privée n'est pas un moyen d'instruction, elle est exécutée en dehors de la procédure et aux frais de la partie mandante lorsqu'elle désire démontrer que l'expert judiciaire est dans la méprise et la défavorise de manière erronée.

390 L'expertise judiciaire (art. 182 ss CPP) a juridiquement la valeur d'une preuve ordinaire[394]. Elle est définie comme une mesure d'instruction par laquelle le juge ou le ministère public conscient de la complexité de l'affaire confie à un ou plusieurs spécialistes – ayant des compétences scientifiques ou techniques – le soin de se prononcer sur des questions de fait ou d'apporter un avis compétent[395]. Etant une mesure d'instruction, l'expertise judiciaire fait partie intégrante du droit de la procédure pénale.

391 La distinction apportée entre expertise privée et judiciaire n'est pas anodine. N'étant pas considérée comme un moyen de preuve, mais comme une simple déclaration faite par une partie au procès, l'expertise privée n'est que peu pertinente dans le contexte probatoire. En revanche, l'expertise judiciaire joue un rôle lors de l'appréciation des preuves par le juge. Nous limitons l'étude à cette mesure d'instruction. L'exégèse de l'expertise doit permettre de déceler les lacunes, les avantages, les inconvénients et la force probante d'un tel mode d'interprétation.

B. Le statut de l'expert

1. Le rôle de l'expert en procédure

a. L'expert et le témoin

392 Par le passé[396], l'expertise a souvent été comprise dans la catégorie des preuves testimoniales, le rapport d'expertise étant le pendant des déclarations faites par les témoins qui exposent les faits marquants et les circonstances utiles à la procédure.

---

[393] ATF 97 I 320, 325; ATF 127 I 73, 82; ATF 132 III 83, 87-88 = JdT 2006 I 334, 336-337 = SJ 2006 I 233, 234; ATF 135 III 670, 677; TF 6B_215/2013 du 27 janvier 2014, c. 1.2; BSK-StPO-HEER, art. 182 N 10; DONATSCH, Jusletter, n° 16; DONATSCH, Kriminalistik 2007, p. 567; MOREILLON, PAREIN-REYMOND, Intro art. 182 ss N 4.

[394] BSK-StPO-HEER, art. 183 N 1; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 174; ZWIEHOFF, p. 16.

[395] MAURER, p. 231; PERRIER DEPEURSINGE, art. 182, p. 231; OBERHOLZER, Strafprozessrechts, p. 293 ss; RIEDO, FIOLKA, NIGGLI, p. 209; SCHMID, Handbuch, p. 396 ss.

[396] PIQUEREZ, Traité de procédure pénale suisse, p. 583-584; RASSAT, p. 423.

393 Même s'il est exact d'affirmer que l'expert effectue des constations sur les faits et événements liés à l'affaire, l'expert est un technicien intervenant dans le cadre d'une procédure pendante grâce à ses connaissances[397].

394 Contrairement au témoin, il n'explique pas ce qu'il a perçu durant la commission de l'infraction, mais il donne une opinion scientifique ou technique motivée et répond à des questions spécifiquement posées par le juge.

395 De surcroît, la personnalité de l'expert n'est pas comparable à celle du témoin. Alors que celui-ci déclare ce qu'il a entendu ou vu, celui-là se limite à ses expériences et aux questions d'ordre scientifique ou technique. Contrairement au statut de témoin qui est reconnu aux uniques personnes qui ont entendu ou vu un élément important, la position de l'expert est interchangeable[398] dès lors que l'aptitude pour répondre à la question est donnée (art. 189 CPP). Ainsi, l'expert peut être remplacé en cours de procédure, soit pour terminer l'expertise – parce que le premier expert a dû se révoquer ou parce qu'il n'a pas tenu ses engagements –, soit pour réaliser une nouvelle expertise, soit encore pour compléter ou clarifier la première expertise.

396 Par conséquent, les déclarations des témoins sont des preuves indirectes, car personnelles, alors que le rapport d'expertise est l'interprétation d'une preuve directe fondée sur l'expérience et les connaissances. L'expert n'a donc pas le statut de témoin[399] et l'expertise n'est pas une preuve testimoniale.

397 Néanmoins, lorsque l'expert est entendu par le ministère public ou le tribunal aux fins de compléter, clarifier ou commenter son rapport d'expertise, les dispositions sur l'audition des témoins lui sont applicables, exception faite de la transmissibilité du procès-verbal reconnu par les tribunaux cantonaux comme étant conforme à la volonté du législateur (art. 187 al. 2 CPP). En procédure, il peut donc être assimilé aux témoins, il n'en devient pas témoin pour autant dès lors qu'il n'a pas constaté personnellement un état de fait. Il reste l'interprète scientifique ou technique et objectif des circonstances de fait.

---

[397] BSK-StPO-HEER, art. 182 N 7; BÜHLER, p. 567; CPP-Commentario-GALLIANI, MARCELLINI, art. 182-191 N 3 et art. 182 N 2; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 164; KAUFMANN, p. 160; MERLE, VITU, T. II, p. 258; PIETH, p. 183-184; PERRIER DEPEURSINGE, art. 182, p. 231; PIQUEREZ, Traité de procédure pénale suisse, p. 380-381; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 282; RIKLIN, Strafprozessordnung, art. 182 N 4.

[398] BSK-StPO-HEER, art. 183 N 4; HAUSER, SCHWERI, HARTMANN, p. 308; JOSITSCH, Strafprozessrechts, p. 108; MERLE, VITU, T. II, p. 258; SCHMID, Handbuch, p. 384-385.

[399] CR-CPP-VUILLE, art. 182 N 1; MERLE, VITU, T. II, p. 258; MOREILLON, PAREIN-REYMOND, Intro art. 182 ss N 1; PERRIER DEPEURSINGE, art. 182, p. 231; SCHMID, Praxiskommentar, art. 182 N 5.

b. L'expert et le juge

398 L'expert n'est pas davantage un juge.

399 La Cour européenne des droits de l'homme rappelle que "[l]es experts ne sont désignés que pour assister le tribunal [ou le ministère public] en lui fournissant des avis éclairés grâce à leurs connaissances spécialisées, sans avoir de fonctions juridictionnelles. Il incombe au tribunal concerné et à ses juges [ou le ministère public] d'apprécier ces avis d'expert, avec l'ensemble des autres informations et preuves pertinentes."[400].

400 Même si l'expertise concerne le fond de l'affaire et que l'expert intervient durant la phase d'instruction ou de procès, il n'est en aucun cas habilité à résoudre des questions juridiques[401]. Il ne peut pas non plus émettre un avis personnel qui ne repose sur aucune base scientifique ou technique. L'expertise ne constitue donc qu'un avis motivé, un élément d'informations sur lequel le juge peut s'appuyer pour rendre sa décision[402] et permettre de respecter la présomption d'innocence.

c. L'expertise et l'avis

401 En ne fournissant pas un avis global, mais s'appuyant sur un cas concret, sur des pièces et des éléments du dossier de procédure pour répondre à une ou des interrogations, l'expertise doit être distinguée de l'avis qualifié.

402 La différenciation entre ces deux types d'avis est prépondérante pour connaître la valeur probatoire de l'expertise.

403 Devant résoudre la problématique de l'administration d'un avis tiré d'une ancienne expertise qui portait sur une question générale, le Tribunal fédéral a déclaré que "*[c]es renseignements*

---

[400] CourEDH, Affaire *D.N c. Suisse*, arrêt du 29 mars 2001, 27154/95, § 53.

[401] ANTOGNINI, p. 3; BÜHLER, p. 574; BSK-StPO-HEER, art. 182 N 4 et art. 184 N 12; CPP-Commentario-GALLIANI, MARCELLINI, art. 182 N 2 et art. 184 N 5; CR-CPP-VUILLE, art. 182 N 8; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 62; JOSITSCH, Strafprozessrechts, p. 108; KAUFMANN, p. 159; MAURER, p. 231; PAYCHÈRE, p. 147; PERRIER DEPEURSINGE, art. 182, p. 231; RIKLIN, Strafprozessordnung, art. 182 N 4; SCHMID, Handbuch, p. 384-385; SCHMID, Praxiskommentar, art. 182 N 2. Infra Partie II, Chapitre 1, I, C, n° 423. Infra Partie II, Chapitre 1, II, B, 2, b, n° 445-449.

[402] BÜHLER, p. 567; CR-CPP-VUILLE, art. 182 N 1; DONATSCH, Kriminalistik 2007, p. 568; HAUSER, SCHWERI, HARTMANN, p. 310; KAUFMANN, p. 220; OBERHOLZER, Strafprozessrechts, p. 293; PERRIER DEPEURSINGE, art. 189, p. 238; PIQUEREZ, Traité de procédure pénale suisse, p. 585; RASSAT, p. 424; RIKLIN, Strafprozessordnung, art. 182 N 4; RODRIGUEZ, p. 22.

sont du même ordre que les explications de caractère général qu'un expert entendu comme "témoin" donne à l'appui d'un rapport écrit. Le juge ne les utilise pas comme preuves, mais comme source d'information [...]"[403]. L'avis scientifique ou technique d'ensemble est donc assimilable aux traités scientifiques ou techniques, mais non à un moyen de preuve. Le juge qui tient compte d'un tel avis appuie sa décision sur la même base que celle relative à la reconnaissance d'une doctrine sans invoquer une preuve concrète de l'affaire.

404 L'expertise, au contraire, doit respecter une certaine procédure pour être valablement administrée au procès (art. 10, 139 ss et 182 ss CPP). Juridiquement, étant liée à une affaire précise, elle doit avoir plus d'impact qu'un simple avis, dès lors que la conclusion spécifique sur un cas d'espèce est plus fiable que le caractère abstrait de l'avis général.

d. L'expert comme auxiliaire de la justice

405 L'expert est un auxiliaire de la justice[404].

406 Par le rôle qu'il joue au sein de l'autorité judiciaire, il est et doit rester indépendant et impartial[405]. Il serait en effet paradoxal qu'un expert – nommé par l'autorité judiciaire et aidant à interpréter les preuves matérielles pour découvrir la vérité – puisse être dépendant et partial, et d'exiger l'impartialité et l'indépendance du juge du fond qui motive une partie de sa décision à l'aide de l'expertise.

407 En conséquence, pour respecter les garanties du procès équitable – tendant à éviter qu'un élément extérieur puisse influer sur le déroulement du procès ainsi que sur le jugement – le juge se doit d'écarter le rapport d'expertise des débats et de procéder au remplacement de l'expert si l'intérêt de la cause le justifie (art. 60 et 184 al. 5 CPP).

---

[403] ATF 107 Ia 212, 214 = JdT 1983 IV 56, 57.

[404] ATF 114 Ia 461, 464; ATF 134 I 159, 163; MOOR, POLTIER, p. 288; PITTELOUD, p. 277.

[405] BSK-StPO-HEER, art. 183 N 19 ss; BÜHLER, p. 567; CPP-Commentario-GALLIANI, MARCELLINI, art. 185 N 1; DONATSCH, Jusletter, n° 8 et 20; DONATSCH, CAVEGN, SJZ 2007, p. 410; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 165; GILLARDIN, JADOUL, p. 124; KAUFMANN, p. 161-163; PERRIER DEPEURSINGE, art. 183, p. 234; PIETH, p. 184; PIQUEREZ, Traité de procédure pénale suisse, p. 386; RIEDO, FIOLKA, NIGGLI, p. 210; RIKLIN, Strafprozessordnung, art. 183 N 1; SCHMID, Handbuch, p. 386-387.

2. Le statut juridique de l'expert

a. Les relations entre l'expert et les parties

408 L'expert judiciaire n'étant pas désigné par les parties, il n'existe pas de relation contractuelle entre eux. Par conséquent, aucune partie ne peut se prévaloir des articles 97 ss CO, notamment du droit de révoquer le contrat.

b. Les relations entre l'expert et la direction de la procédure

409 Les relations juridiques entre la direction de la procédure et l'expert sont plus complexes à définir.

410 Le Tribunal fédéral a examiné la qualification des relations juridiques entre l'expert et l'autorité publique[406]. En s'appuyant sur l'avis de plusieurs auteurs de doctrine[407], il a reconnu que l'expert était lié par un rapport de droits et d'obligations similaire au contrat de mandat (art. 394-418*v* CO)[408] ou au contrat d'entreprise (art. 368 CO) lorsque le résultat de l'expertise est susceptible d'être vérifié selon des critères objectifs[409]. Néanmoins, la Cour a tempéré ses propos en déclarant que les litiges entre l'autorité publique et l'expert n'étaient pas du ressort du droit privé, mais bien du droit public[410].

411 La position du Tribunal fédéral se base à juste titre sur la qualité du mandant. Dans le cadre de l'expertise judiciaire, le mandant est le juge ou toute autre autorité publique compétente qui agit en tant que détenteur de la puissance publique[411].

412 En procédure pénale, la direction de la procédure veille à la bonne administration de la justice et au respect des droits procéduraux. L'expert désigné est un auxiliaire qui veille à aider la direction de la procédure dans l'accomplissement d'une de ses tâches, soit l'établissement des faits.

---

406 ATF 114 Ia 461, 464 = JdT 1990 I 182, 185; ATF 127 III 328, 330 = JdT 2001 I 254, 256-257; ATF 134 I 159, 160.

407 GAUTSCHI, art. 394 N 34*b*; KNAPP, p. 538.

408 ATF 114 Ia 461, 464= JdT 1990 I 182, 185; ATF 134 I 159, 164.

409 ATF 127 III 328, 330 = JdT 2001 I 254, 256-257; RJN 2007 126, 132.

410 ATF 134 I 159, 165 = JdT 1990 I 182, 185; ATF 134 I 159, 163; PITTELOUD, p. 279.

411 ATF 114 Ia 461, 464= JdT 1990 I 182, 185; ATF 134 I 159, 164; GAUTSCHI, art. 394 N 34*b*; KNAPP, p. 538.

413 En outre, le statut de l'expert se rapproche de celui du magistrat et de toute personne exerçant une fonction au sein de l'autorité pénale. Il est passible de récusation (art. 56 ss CPP), il peut être l'auteur ou la victime d'un acte de corruption (art. 322*ter*-322*sexties* CP), et, étant assimilable à la notion de fonctionnaire (art. 110 al. 3 CP)[412], il est tenu au secret de fonction (art. 320 CP). Ces éléments confirment que l'expert doit être considéré comme un agent public ayant une relation de droit public avec la direction de la procédure.

414 Il reste encore à déterminer de quel type d'acte il s'agit. D'après Pierre Moor et Etienne Poltier[413] ainsi que Thierry Tanquerel[414], l'Etat peut créer un lien juridique, notamment par une décision, un contrat de droit administratif ou un contrat de droit privé[415]. Ce dernier type d'acte n'entre pas en considération puisque les rapports entre l'expert et l'autorité pénale sont de droit public.

415 Bernard Bertossa[416] considère qu'il s'agirait plutôt d'un contrat de droit administratif puisque l'expert doit effectuer une tâche publique en sa qualité d'auxiliaire de la justice niant toutefois l'importance du rapport de subordination[417]. Néanmoins, cet auteur émet des doutes sur la qualification de contrat dès lors que l'expert, ne pouvant pas refuser sa mission, ne bénéficie pas d'une autonomie de sa volonté, requise dans le cadre d'un contrat[418]. Pierre Moor et Etienne Poltier définisse la décision administrative lorsque les droits et devoirs du tiers sont formulés abstraitements[419], ce qui est le cas lors de la nomination d'un expert. A notre avis, l'activité de l'expert judiciaire étant réglée exclusivement dans une loi, ce qui ne laisse aucune place à la négociation des prestations, il semble que son activité relève plus d'un contrat administratif au quel s'applique les règle du mandat ou d'entreprise[420].

416 En tant qu'auxiliaire de la justice désigné par la direction de la procédure, l'expert est responsable de l'exécution de son travail et de sa conformité avec les règles de l'art. Il répond seul de la mauvaise réalisation de l'expertise ou des erreurs qu'il a pu commettre. Mentionnons encore que le spécialiste peut engager sa responsabilité pénale – commission

---

412 ATF 125 II 541, 544; TF 1P.787/2005 du 6 juin 2006, c. 1.7; HAUSER, SCHWERI, HARTMAN, p. 310; SCHMID, Praxiskommentar, art. 184 N 11 et 13-14; StPO-DONATSCH, art. 184 N 29.

413 MOOR, POLTIER, p. 421.

414 TANQUEREL, p. 234-235.

415 MOOR, POLTIER, p. 421; TANQUEREL, p. 234-235; WIEDERKEHR, RICHLI, p. 791, 1006 et 1034.

416 BERTOSSA, p. 399.

417 *Contra* ATF 102 II 57.

418 BERTOSSA, p. 398.

419 MOOR, POLTIER, p. 424-426.

420 PERRIER DEPEURSINGE, art. 184, p. 235-236; StPO-DONATSCH, art. 182, N 12.

des infractions prévues aux articles 307, 320, 322*quater* et 322*sexties* CP – ou civile pour acte illicite[421].

417 En revanche, l'expert ne doit pas fidélité au juge, bien au contraire. L'expert ne travaille pas pour le juge, mais pour la justice en collaborant uniquement à la recherche de la vérité matérielle[422].

C. La portée de l'expertise

418 Historiquement, le juge a eu recours ponctuellement à des spécialistes lorsqu'une question était soulevée et n'entrait pas dans les limites de ses connaissances. Ainsi, les arpenteurs à Rome mesuraient les terres, les huissiers-priseurs estimaient les biens et les jardiniers de Constantinople évaluaient les légumes[423].

419 Dans le domaine pénal, l'usage de l'expertise s'est forgé une place lorsque la justice s'est tournée vers la science et la technique pour comprendre et interpréter les faits de l'affaire en cause. Le recours à l'expert est devenu de plus en plus fréquent dès le XIX^{e} siècle[424]. Aujourd'hui plus qu'hier, les techniciens ou scientifiques jouent un rôle toujours plus éminent dans l'administration des preuves, la "phase sentimentale" de la preuve morale se transformant en "phase scientifique". Plus la science se développe, plus les tribunaux recourent à des spécialistes pour être informés de manière adéquate sur les questions d'ordre scientifique ou technique[425].

420 L'expertise peut servir à établir un état de fait grâce aux connaissances spécifiques de l'expert, apprécier un état de fait grâce à ces connaissances particulières et aux règles générales d'expérience ou simplement communiquer des règles générales d'expérience[426].

421 La complexité des indices matériels empêche souvent leur utilisation immédiate et fournit rarement un résultat non équivoque. Dans de nombreux cas, les juristes ne sont pas aptes à interpréter et faire "parler" les indices. L'expert permet donc à l'autorité pénale de concrétiser

---

[421] BETTEX, p. 281-288; StPO-DONATSCH, art. 185 N 9.

[422] BÜHLER, p. 567; CR-CPP-VUILLE, art. 182 N 1; DONATSCH, Kriminalistik 2007, p. 568; HAUSER, SCHWERI, HARTMANN, p. 310; KAUFMANN, p. 220; OBERHOLZER, Strafprozessrechts, p. 293; PERRIER DEPEURSINGE, art. 183, p. 234; PIQUEREZ, Traité de procédure pénale suisse, p. 503; RASSAT, p. 42; ZWIEHOFF, p. 16.

[423] PIQUEREZ, Traité de procédure pénale suisse, p. 382.

[424] MERLE, VITU, T. II, p. 258; ZOLLINGER, p. 570.

[425] BSK-StPO-HEER, art. 182 N 1; BÜHLER, p. 574; RASSAT, p. 419; RODRIGUEZ, p. 22.

[426] BETTEX, p. 7.

la maxime d'office en investiguant des faits impossibles à apprécier par manque de connaissances.

422 A partir du moment où le ministère public ou le juge estime qu'il n'a pas les aptitudes requises pour répondre à une problématique, il fait appel à un expert. Il est notoire que le spécialiste donne son concours à la justice dans le domaine médical, biologique, chimique ou technique[427]. Ces dernières années, l'intervention de la police scientifique comme expert est quasi systématique pour permettre l'analyse des traces, la détection et l'identification des empreintes digitales, l'analyse ADN, etc. Depuis peu, un nouveau domaine d'expertise se développe avec l'évolution de l'informatique et l'utilisation de nombreux appareils techniques complexes (expertises en informatique, expertises et analyses mathématiques, expertises de localisation, etc.). La direction de la procédure recourt ainsi à l'expertise lorsqu'elle l'estime nécessaire, encore faut-il que le domaine des connaissances professionnelles utiles à l'établissement ou à l'exploitation d'un fait soit sûr et incontesté. L'accomplissement de ces deux conditions permet de reconnaître aux conclusions de l'expert une valeur scientifique ou technique suffisante pour être admises à la procédure. Si tel est le cas, le spécialiste entre en jeu, soit pour aider l'autorité pénale compétente lorsque l'état d'un fait n'est identifiable qu'avec son concours, soit parce qu'un élément est identifiable sans connaissances professionnelles, mais qu'il nécessite un savoir et de l'expérience pour être apprécié[428].

423 Ainsi, l'expertise et ses conclusions apparaissent comme un moyen adéquat pour découvrir et apprécier certaines preuves[429]. Ce moyen d'instruction fournit une base solide au juge du fond pour déterminer sa conviction sur l'existence, l'inexistence d'un fait ou sur l'interprétation à donner à un indice retrouvé sur les lieux de l'infraction. En revanche, l'expert ne doit pas s'arroger les compétences appartenant aux magistrats. Conformément à l'adage *iura novit curia*, le juge ne peut pas déléguer ses pouvoirs juridictionnels[430], notamment ceux relatifs à l'appréciation des preuves ou au droit applicable. Le technicien est appelé à ne régler que des questions de fond, soit des questions extrajudiciaires. Il doit répondre complètement et uniquement à la ou aux questions précisément posée(s) par le magistrat. Ces interrogations se limitent à l'éclaircissement de notions scientifiques ou

[427] BSK-StPO-HEER, art. 182 N 2; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 175; KAUFMANN, p. 157; PIQUEREZ, Traité de procédure pénale suisse, p. 583.

[428] BSK-StPO-HEER, art. 182 N 1; CR-CPP-VUILLE, art. 182 N 6; CPP-Commentario-GALLIANI, MARCELLINI, art. 182-191 N 2; DONATSCH, Jusletter, n° 7; DONATSCH, Kriminalistik 2007, p. 566; HAUSER, SCHWERI, HARTMANN, p. 308; KAUFMANN, p. 157-158; PIQUEREZ, Traité de procédure pénale suisse, p. 380; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 280; RIKLIN, Strafprozessordnung, art. 182 N 1; SCHMID, Handbuch, p. 384.

[429] DONATSCH, Jusletter, n° 3; ZWIEHOFF, p. 26 et 33.

[430] BSK-StPO-HEER, art. 182 N 4; GILLARDIN, JADOUL, p. 128; KAUFMANN, p. 159; PIETH, p. 184; PIQUEREZ, Traité de procédure pénale suisse, p. 384.

techniques concernant un aspect de fait du procès dans le strict respect de la présomption d'innocence, du procès équitable et des conditions de forme et de fond de l'expertise.

II. L'expertise en procédure pénale

A. La saisine de l'expert

424 En vertu de la législation fédérale, le juge est contraint de recourir à un spécialiste lorsqu'il y a un doute sur la responsabilité du prévenu (art. 20 CP), lorsque l'état mental du prévenu doit être déterminé (art. 56 al. 3 CP) ou encore lorsqu'il se justifie de fixer le taux d'alcoolémie d'un conducteur (art. 55 LCR et art. 142*a* et 142*b* OAC)[431]. Dans de telles circonstances, le droit pénal de fond détermine les modalités à respecter pour faire intervenir un expert (art. 56 al. 4 et 4*bis*, art. 64*c* al. 5 et 359 CP). Le recours systématique à un médecin spécialiste est également prévu en cas de mort suspecte (art. 253 CPP)[432].

425 Quand il s'agit d'analyser et d'interpréter une preuve matérielle ou d'expliciter un principe, le caractère obligatoire de l'expertise disparaît. En principe, l'expertise est ordonnée d'office par l'autorité pénale lorsque les conditions de l'art. 182 CPP sont remplies. Cependant, une partie à la procédure peut demander une expertise. Le ministère public ou le tribunal apprécie toutefois souverainement l'opportunité de désigner un expert selon que les circonstances exigent des connaissances techniques spécifiques (art. 182 CPP). Le magistrat peut donc refuser de nommer un expert sans violer les droits de la défense si l'expertise apparaît d'emblée comme inutile[433]. La large manœuvre de l'autorité pénale quant à la désignation d'un expert n'est pas sans risque dès lors qu'elle est seule à décider de la nécessité d'y recourir.

426 Mentionnons encore que dans le cadre de l'utilisation des nouvelles technologies, la désignation optionnelle n'est pas une possibilité anodine pour concrétiser la maxime d'office qui veut que les faits soient investigués[434].

---

[431] JOSITSCH, Strafprozessrechts, p. 109; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 174; PIQUEREZ, Traité de procédure pénale suisse, p. 385-386; SCHMID, Handbuch, p. 386; SCHMID, Praxiskommentar, art. 182 N 3.

[432] BOBAY, RUDER, p. 32.

[433] ATF 131 I 153, 157-158.

[434] CR-CPP-VUILLE, art. 182 N 5; HAUSER, SCHWERI, HARTMANN, p. 308; StPO-DONATSCH, art. 182 N 29.

B. L'expertise judiciaire facultative

1. Le choix de l'expert

a. Le droit de consultation des parties

427 En droit pénal, le choix et la désignation du ou des experts sont de la compétence exclusive de la direction de la procédure – le ministère public ou le juge du fond – lorsqu'elle l'estime nécessaire (art. 182 CPP) pour pallier les lacunes du savoir de la justice[435]. Par voie de décision, elle désigne le nombre d'experts appelés à aider la justice, leur nom et leurs tâches.

428 L'art. 6 § 1 CEDH, l'art. 14 § 1 Pacte II et l'art. 29 al. 1 et 2 Cst garantissent le droit à un procès équitable dont l'un des éléments essentiels est le caractère contradictoire de la procédure et le droit d'être entendu[436]. Cependant, aucune de ces bases légales n'accorde aux parties le droit de choisir l'expert ou de se prononcer sur le choix du juge[437].

429 La jurisprudence de la Cour européenne a spécifié que la garantie au procès équitable et son corollaire – le droit à la contradiction – ne sont pas des principes généraux et abstraits[438]. La direction de la procédure n'est donc pas obligée d'entendre les parties sur le choix de l'expert et/ou les questions posées, il suffit que celles-là puissent participer de manière adéquate à un moment donné de la procédure avant qu'une décision ne soit prise[439].

430 En revanche, les exigences d'impartialité et d'indépendance – éléments du procès équitable – permettent aux parties d'exiger de l'autorité de recours la récusation de l'expert[440]. Au surplus, les parties ont la possibilité de formuler des observations, de demander des compléments ou des clarifications (art. 188-189 CPP)[441]. Ainsi, les parties ont la possibilité de

---

[435] ANTOGNINI, p. 3; CR-CPP-VUILLE, art. 182 N 22 ss; De 29 à l'unité, p. 107.

[436] ATF 127 I 196, 198; ATF 130 I 388, 393; CourEDH, Affaire *Lobo Machado c. Portugal*, arrêt du 20 février 1996, 15764/89, § 31-32; CourEDH, Affaire *Vermeulen c. Belgique*, arrêt du 20 février 1996, 19075/91, § 33; CourEDH, Affaire *Nideröst-Huber c. Suisse*, arrêt du 18 février 1997, 18990/91, § 24; CourEDH, Affaire *Mantovanelli c. France*, arrêt du 18 mars 1997, 21497/93, § 33; CourEDH, Affaire *Steel et Morris c. Royaume-Uni*, arrêt du 15 mai 2005, 68416/01, § 62; CourEDH, Affaire *Louis c. France*, arrêt du 14 février 2007, 44301/02, § 31-38.

[437] TF 6P.39/2006 du 30 août 2006, c. 3; HAUSER/SCHWERI/HARTMANN, p. 309.

[438] CourEDH, Affaire *Kerojärvi c. Finlande*, arrêt du 19 juillet 1995, 17506/90, § 42; CourEDH, Affaire *Mantovanelli c. France*, arrêt du 18 mars 1997, 21497/93, § 33; CourEDH, Affaire *Susanna Ros Westlund c. Islande*, arrêt du 6 décembre 2007, 42628/04, § 33.

[439] ATF 99 Ia 42, 46; ATF 125 II 591, 604; ATF 131 II 680, 683-684.

[440] ATF 126 I 68, 73; TF 1B_488/2011, c. 1.1 = Forumpoenale 2012 p. 285.

[441] Infra Partie II, Chapitre 1, III, C, 3, n° 471 ss.

participer adéquatement à la procédure, ce qui est suffisant pour respecter les garanties du Pacte II, de la Convention européenne des droits de l'homme et de la Constitution.

431 Le Code de procédure pénale va plus loin dans la protection de la garantie au procès équitable lors de la désignation de l'expert en donnant un droit de consultation aux parties. Afin d'éviter une demande de récusation subséquente (art. 56 ss CPP) et d'économiser la procédure, le magistrat qui rend la décision de nomination entend les parties sur son futur choix (art. 184 al. 3 CPP) et prend en considération leurs propositions. Néanmoins, la direction de la procédure n'est pas obligée de tenir compte de l'avis exprimé par les parties[442].

432 La faculté offerte aux parties de se prononcer sur le choix de l'expert et les questions qui lui sont posées souffrent d'une exception dans les cas d'actes d'enquête routiniers pour lesquels il existe des protocoles d'analyse préétablis (art. 184 al. 3 phr. 2 CPP)[443]. Le texte légal souffre de quelques imprécisions, voire d'incohérences.

433 En premier lieu, l'interprétation littérale de la loi conduit à ce que le travail effectué avant ou après l'analyse n'est pas soumis à l'exception. Au contraire, Jürg Sollberger[444] estime quant à lui que tous les actes réalisés dans l'urgence – et non pas selon le caractère routinier – sont concernés. Cette interprétation n'est cependant pas fidèle à la lettre de la loi puisque l'art. 184 al. 3 CPP parle de "*déterminer*", "*établir*" et "*prouver*", ce qui n'équivaut pas à "prélever". Si seuls les actes réalisés dans l'urgence de la préservation de la scène étaient concernés, l'analyse serait soumise au régime ordinaire. La volonté du législateur ne semble pas être celle-là. Néanmoins, nier l'application de l'exception pour le simple prélèvement peut être délicat puisqu'un temps précieux peut être perdu d'ici à ce que le prévenu et toutes les parties à la procédure se prononcent sur le choix de l'expert.

434 Il semble correct de s'écarter de la lettre de la loi et de la volonté du législateur en considérant le prélèvement et la phase après analyse comme entrant dans le cadre de la loi pour permettre à l'expert d'analyser et d'interpréter ce qu'il a pu constater par une observation directe de la scène de crime. Au surplus, la limite imposée par le simple fait qu'il s'agisse d'opérations de routine n'est également pas satisfaisante. Il est préférable de s'accorder sur l'existence ou non d'un laboratoire ou de personnes accréditées qui suivent un protocole d'analyse préétablis pour garantir la qualité des résultats sans que la consultation des parties soit nécessaire[445].

---

[442] CR-CPP-VUILLE, art. 184 N 17; HAUSER, SCHWERI, HARTMANN, p. 336.

[443] SCHMID, Praxiskommentar, art. 184 N 14; VUILLE, TARONI, RPS 2011, p. 165.

[444] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 176.

[445] VUILLE, TARONI, RPS 2011, p. 167.

435 En second lieu, l'exception de l'art. 184 al. 3 phr. 2 CPP nous semble dangereuse quant à l'importance portée aux questions posées à l'expert. Cette base légale empêche les parties de se prononcer sur les questions. Du point de vue scientifique, l'élaboration de la question est un élément essentiel pour minimiser les risques d'erreur lors de la prononciation des résultats[446]. Pour qu'un moyen de preuve soit correctement évalué de manière indépendante et transparente, l'évaluation par hypothèse est la méthode la plus adéquate. Le simple fait d'exposer à l'expert un autre avis ou questionnement permet d'élargir le champ des possibilités pour l'investigation. Plus les questions ouvrent une vision des événements, plus l'expert est amené à se positionner de manière neutre[447]. C'est pourquoi, il est important que les parties puissent émettre des propositions quant aux questions à poser. La possibilité offerte aux parties de se prononcer sur l'expertise réalisée et de demander des compléments ou des clarifications (art. 185-186 CPP) n'est pas suffisante pour réparer la perte de contradiction au moment du choix des questions. L'atteinte psychologique de l'expert est en effet déjà réalisée et son ouverture à une autre vision paraît *a posteriori* difficile.

436 En accord avec Franco Taroni et Joëlle Vuille[448], il nous apparaît que l'exception de l'art. 184 al. 3 CPP est une fausse bonne idée.

b. Les conditions pour être expert

437 L'expert doit être une personne physique (art. 183 al. 1 CPP), capable, non récusable et qui possède les connaissances techniques et/ou scientifiques nécessaires (art. 183 al. 1 *in fine* CPP). A noter qu'un expert a un certain nombre de responsabilités dont il répond personnellement. Un professionnel rattaché à une personne morale n'est pas d'emblée exclu. Il peut être désigné par mandat, mais il est alors soumis aux obligations imparties aux experts et non à celles de son employeur[449].

438 L'expert devant élucider la ou les problématiques qui lui sont posées et l'autorité judiciaire devant pouvoir s'appuyer sur l'opinion du spécialiste pour rendre sa décision, les aptitudes techniques ou scientifiques sont une condition *sine qua non* impliquant que les connaissances professionnelles de l'expert ne doivent pas être remises en question par les parties. Contrairement à la France, il n'existe en Suisse aucune liste officielle d'experts

[446] INMAN, RUDIN, p. 248; VUILLE, Thèse, p. 66.

[447] INMAN, RUDIN, p. 250.

[448] VUILLE, TARONI, RPS 2011, p. 164ss.

[449] A ce sujet: CPP-Commentario-GALLIANI, MARCELLINI, art. 183 N 1 et art. 185 N 1 ; MOREILLON, PAREIN-REYMOND, art. 183 N 4; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 282.

judiciaires restreignant le choix du juge ou du ministère public, exception faite de certains domaines où la Confédération et les cantons peuvent recourir à des experts permanents ou officiels[450]. Le magistrat est donc libre de désigner un expert de nationalité suisse ou étrangère pour autant que, selon ses sources, il possède les connaissances utiles à l'élucidation des questions posées et qu'il connaisse les règles procédurales régissant l'établissement d'une expertise[451]. La préférence doit être portée sur un spécialiste pouvant comprendre aisément la situation légale et dont la terminologie juridique ne lui est pas étrangère.

439 Pour assurer la capacité et l'aptitude d'un expert, la Chambre suisse des experts techniques et scientifiques à Lausanne, l'Union Technique Suisse (UTS) à Zurich et d'autres unions professionnelles établissent périodiquement des listes, dans le but de faciliter la prise de décision du magistrat concernant la désignation d'un technicien[452]. La Chambre suisse a en outre créé un certificat – Swiss Expert Certification (SEC)[453] – accrédité ISO 17024[454] garantissant la compétence, l'expérience et l'impartialité dans le domaine d'activité de l'expert.

440 Une fois désigné, le choix de la direction de la procédure s'étant porté sur lui et non sur un autre spécialiste, l'expert désigné répond personnellement de l'exécution de l'expertise. La substitution n'est possible que si elle est permise explicitement ou tacitement (art. 184 al. 2 let. b CPP). Dans le cas contraire, si l'expert délègue sa tâche à une autre personne, l'expertise est exclue de l'appréciation des preuves (art. 141 al. 2 CPP)[455]. Dans une telle hypothèse, une nouvelle expertise est réalisée incluant *a priori* la désignation d'un nouvel expert, puisque la violation du devoir et les risques d'impartialité entachent le spécialiste originellement désigné. En revanche, s'il ne s'agit pas de déléguer la mission ou de constituer une pluralité d'experts à l'insu de la direction de la procédure, la consultation d'un autre spécialiste par l'expert n'est pas d'emblée exclue. Généralement, il est admis que l'expert recoure – sous sa responsabilité (art. 185 al. 1 CPP) – au concours d'un technicien plus spécialisé[456] lorsqu'il n'a pas les connaissances techniques sur un point précis, utile et

[450] A ce sujet, voir notamment: art. 8 Loi sur les profils d'ADN; art. 25 LaCP/GE.

[451] DONATSCH, Jusletter, n° 40; KAUFMANN, p. 164.

[452] BETTEX, p. 104; KAUFMANN, p. 164.

[453] Informations disponibles sur le site internet du SEC : http://www.experts-certification.ch/fr/frhome [consulté le 08.05.2016].

[454] ISO/IEC 17024:2003 "Evaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes".

[455] BSK-StPO-HEER, art. 183 N 11-12; KAUFMANN, p. 222.

[456] BOBAY, RUDER, p. 32; BSK-StPO-HEER, art. 183 N 11-12 et art. 184 N 11; GILLARDIN, JADOUL, p. 135-136; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 177; SCHMID, Handbuch, p. 392.

nécessaire à la rédaction de l'expertise. N'étant pas mandaté expressément par la direction de la procédure, l'avis fourni par le second expert ne reste qu'un élément de la motivation générale du rapport d'expertise officielle sans occuper une place prépondérante.

2. Le mandat d'expertise

a. La forme

441 La mise en œuvre d'une expertise judiciaire facultative fait suite à l'élaboration d'un mandat écrit (art. 184 al. 2 CPP) ou en cas d'urgence d'un mandat oral et consigné au procès-verbal (art. 77 CPP)[457] par le ministère public ou le juge désireux d'obtenir un avis compétant. La forme du mandat d'expertise étant une prescription d'ordre[458], en cas de non-respect, l'expertise demeure exploitable (art. 141 al. 3 CPP).

442 L'ordonnance de mise en œuvre d'une expertise étant considérée comme une décision au sens de l'art. 80 CPP, le mandat comprend la nomination de la personne experte, la ou les tâches à accomplir[459], les droits, obligations et responsabilités de l'expert ainsi que la date de la demande et le délai à respecter (art. 184 al. 2 let. a à f CPP). Cette dernière indication est essentielle pour garantir le principe de célérité voulant que le jugement soit rendu dans un délai convenable (art. 5 al. 1 CPP). Si un délai pour fournir les conclusions n'est pas fixé, le juge risque de ne pas être en mesure de rendre sa décision – à défaut d'obtenir les informations utiles pour apprécier correctement les faits – dans un délai raisonnable et sans retard injustifié.

443 Sans mandat, le nom de l'expert, les obligations et les tâches n'étant pas connus, la saisine de l'expert est impossible. Cette décision d'octroi d'un mandat est donc fondamentale pour actionner cette mesure d'instruction qu'est l'expertise judiciaire facultative des moyens de preuves.

---

457 Message, CPP, p. 1192.

458 GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-MAURER, p. 401; Message, CPP, p. 1192; MOREILLON, PAREIN-REYMOND, art. 184 N 8; Polizeiliche Ermittlung-ARMBRUSTER, VERGÈRES, p. 287; SCHMID, Handbuch, p. 388.

459 MOREILLON, PAREIN-REYMOND, art. 184 N 2; SCHMID, Handbuch, p. 390; SCHMID, Praxiskommentar, art. 184 N 1 et 5 ss.

b. Le contenu

444 L'expert tire sa légitimité et ses pouvoirs du mandat rédigé par la direction de la procédure comprenant la ou les questions posées. Le spécialiste devant se focaliser à répondre aux incompréhensions ou incertitudes des magistrats, le libellé de l'objet est donc essentiel pour délimiter avec précision le champ de l'expertise.

445 La mission de l'expert est essentiellement technique. Elle ne porte que sur des questions de faits requérant des aptitudes professionnelles. Le rôle du spécialiste se borne à analyser et exposer son avis objectif en s'appuyant sur des observations et expérimentations rendant sa construction des événements plus tangible[460]. Contrairement au témoin ou à la personne appelée à donner des renseignements, l'expert apporte une réponse exacte à une question posée avec pour unique appui la science ou la technique sans se fonder sur la mémoire ou les simples connaissances humaines.

446 L'objet de l'expertise peut être de deux sortes: la justice doit se fonder sur des faits connus dont un point est contestable et nécessite des connaissances professionnelles pour en établir la véracité[461], ou la justice a besoin de clarifier l'accomplissement des conditions légales et demande le concours de l'expert pour constater si un fait est donné ou non. Qu'il s'agisse de connaître de manière exacte les faits déjà présentés ou de définir la situation légale, l'expertise vise à interpréter scientifiquement ou techniquement l'état de fait, voire à le constater entièrement ou en partie. En aucun cas la direction de la procédure ne peut poser une question juridique et l'expert ne doit jamais s'exprimer par des considérants juridiques. Dans le cas contraire, la direction de la procédure a l'interdiction de se fonder sur l'opinion de l'expert.

447 En outre, le libellé de la mission d'expertise est soumis à l'exigence de la neutralité. Il doit être libre de toutes suggestions[462] et ne pas contenir la réponse attendue. Par exemple, dans un procès pour meurtre avec profilage ADN, la question de l'expertise: "*Est-ce bien l'ADN du prévenu qui a été retrouvé sur les lieux du meurtre?*" suggère la position de l'autorité judiciaire quant à la culpabilité du suspect. Elle est inacceptable. La préférence doit être portée à un libellé plus neutre "*L'ADN retrouvé sur les lieux du crime est-il identifiable?*", puisque légalement ce qui importe est d'identifier la trace ADN et non pas de juger coupable à tout prix le prévenu.

---

[460] CR-CPP-VUILLE, art. 182 N 6; KAUFMANN, p. 165; PIETH, p. 183-184; StPO-DONATSCH, art. 182 N 21.

[461] PIQUEREZ, Traité de procédure pénale suisse, p. 380; ZWIEHOFF, p. 33.

[462] CPP-Commentario-GALLIANI, MARCELLINI, art. 184 N 5; KAUFMANN, p. 166-167; ZWIEHOFF, p. 33.

448 L'expert doit généralement répondre à toutes les questions posées par l'autorité pénale dans l'hypothèse où elles ne relèvent pas du droit ou ne sont pas suggestives. Néanmoins, il nous faut tempérer cette obligation. Sans s'en rendre compte, le ministère public ou les tribunaux posent des questions auxquelles les experts ne peuvent simplement pas répondre en vertu de la répartition des rôles. Notamment, l'expertise réalisée à la suite de l'analyse des traces dactyloscopiques permet d'évaluer la preuve à savoir si un lien est créé entre la trace et un suspect, mais ne permet en aucun cas de déterminer les circonstances de fait qui expliquent la présence de ladite trace sur les lieux de l'infraction. Les connaissances contextuelles et les hypothèses de travail pouvant expliquer la présence d'une preuve sur un lieu d'infraction sont du ressort exclusif de l'autorité pénale. Demander à un expert d'expliquer la présence d'une trace sur la scène de crime est une question récurrente nous amenant à constater un transfert partiel de responsabilité du juriste sur l'expert.

449 En outre, le terme "*juger*" de l'art. 182 CPP est trompeur. Mis à part les questions de culpabilité et de qualification juridique d'un comportement, l'expert ne doit pas apprécier une preuve[463]. En tant qu'auxiliaire de la justice, il aide le juge à exercer sa tâche en mettant ses connaissances au service de la justice pour apprécier ou constater l'état de fait, mais en aucun cas il ne juge.

3. La récusation et la révocation

a. Le principe

450 L'administration de la justice n'est crédible et n'a d'autorité que si les personnes impliquées dans la procédure recherchent la vérité matérielle. Pour cette raison, l'expert doit être loyal dans la recherche de la preuve et son administration, être objectif, être rigoureux dans ses démarches, soit être impartial[464].

451 L'implication de tout sentiment personnel mettant en doute l'objectivité doit être d'emblée exclue. En cas de suspicion quant à la subjectivité du spécialiste, des vérifications doivent être entreprises pouvant aboutir à l'écartement de l'expert par l'application des règles de la

[463] SCHMID, Handbuch, p. 384-385.

[464] ATF 120 V 357, 367; BSK-StPO-HEER, art. 183 N 19 ss; BÜHLER, p. 567; CPP-Commentario-GALLIANI, MARCELLINI, art. 185 N 1; DONATSCH, Jusletter, n° 8 et 20; DONATSCH, CAVEGN, SJZ 2007, p. 410; GILLARDIN, JADOUL, p. 124; KAUFMANN, p. 161-163; MOREILLON, PAREIN-REYMOND, art. 183 N 13; PIETH, p. 184; PIQUEREZ, Traité de procédure pénale suisse, p. 386; RIKLIN, Strafprozessordnung, art. 183 N 1; SCHMID, Handbuch, p. 386-387. Supra Partie II, Chapitre 1, I, C, 2, n° 467-470.

récusation visant à garantir la confiance en la justice (art. 6 § 1 CEDH, art. 14 Pacte II et art. 30 al. 1 Cst confirmés par les art. 183 al. 3 CPP *cum* art. 56 ss CPP).

452 Les motifs de récusation sont de deux ordres: particuliers (art. 56 let. b à e CPP) ou généraux (art. 56 let. a et f CPP) englobant les causes de récusation dites absolues ou relatives[465].

453 Les causes absolues impliquent que l'expert est *eo ipso* dans l'incapacité de remplir sa charge, notamment parce qu'il existe un lien de parenté avec le magistrat de fond ou l'une des parties, voire que l'expert lui-même est impliqué matériellement ou officiellement dans l'affaire.

454 Les causes relatives ne font l'objet d'une demande de récusation déliant l'expert que si l'autorité publique compétente reconnaît l'application d'un des motifs prévus à l'art. 56 CPP.

455 Relevons encore que les motifs généraux – énoncés sous "*autres motifs*" (art. 56 let. f CPP) – font référence aux causes pouvant embarrasser un expert[466]. Notamment, lorsque l'expert est adhérent d'une doctrine déterminée, mais contestable, et s'est prononcé en public sur cette opinion, lorsqu'il exerce une fonction au sein de l'autorité pénale, lorsqu'il a été saisi par le passé[467] – par exemple, si il a été le médecin traitant d'une des parties – ou si son rapport a conduit à l'ouverture d'une instruction[468]; lorsqu'il a déjà participé à l'administration des preuves à la cause en tant que partie ou qu'expert privé[469]; lorsqu'il entretient un contact étroit avec un expert préalablement récusé[470] ou toute personne étant personnellement impliquée, le choix du magistrat ne peut pas se porter sur ce spécialiste (art. 56 CPP). *A contrario*, l'expert qui doit se prononcer sur l'avis d'un collègue travaillant dans le même institut[471], qui a été entendu comme témoin ou qui intervient une deuxième fois en première instance[472], voire est appelé également en deuxième instance[473] n'est pas récusable pour ces

---

[465] Message, CPP, p. 1126.

[466] KAUFMANN, p. 161; SCHMID, Praxiskommentar, art. 56 N 14.

[467] ATF 94 I 417, 425 = JdT 1970 I 383; ATF 124 I 170, 175.

[468] ATF 120 V 357, 365; CourEDH, Affaire *Bönisch c. Autriche*, arrêt du 06 mai 1985, 8658/79, § 32; CourEDH, Affaire *Stoimenov c. L'ex-République yougoslave de Macédoine*, arrêt du 05 avril 2007, 17995/02, § 39-40.

[469] ATF 125 II 541, 544-545; BÜHLER, p. 569; DONATSCH, Jusletter, n° 32

[470] ATF 97 I 320, 323-324; ATF 119 Ia 221, 226; ATF 120 Ia 184, 187 = JdT 1996 II 67, 70; PERRIER DEPEURSINGE, art. 183, p. 234.

[471] CourEDH, Affaire *Brandstetter c. Autriche*, arrêt du 28 août 1991, 11170/84, 12876/87 et 13468/87, § 44; CourEDH, Affaire *Mantovanelli c. France*, arrêt du 18 mars 1997, 21497/93, § 33; CourEDH, Affaire *Sara Lind Eggertsdottir c. Islande*, arrêt du 05 juillet 2007, 31930/04, § 47-53.

[472] DONATSCH, Jusletter, n° 26; HAUSER, SCHWERI, HARTMANN, p. 309.

[473] DONATSCH, Jusletter, n° 24; HAUSER, SCHWERI, HARTMANN, p. 309; SCHMID, Handbuch, p. 386-387.

motifs. Quant aux fonctionnaires de police, ils peuvent être désignés comme experts à la seule condition de ne pas avoir d'implication personnelle dans l'affaire répressive[474].

456 En conséquence, le motif de récusation importe peu qu'il soit absolu ou relatif, particulier ou général, personnel, affectif ou professionnel, la récusation n'est admissible que si un motif valable – démontrant le parti pris ou l'incapacité du spécialiste – existe, sans quoi la justice serait sérieusement entravée et la société dans son ensemble manquerait de confiance[475]. Si un tel motif existe, l'expert doit l'annoncer en temps utile à la direction de la procédure (art. 57 CPP) pour éviter les conséquences d'annulation et de répétition de l'expertise (art. 60 CPP). Dans l'hypothèse où le spécialiste ne se récuse pas, alors qu'il y a motif, une partie au procès peut en faire la demande sans délai après avoir pris connaissance du motif de récusation (art. 58 CPP) – soit le plus rapidement possible et non pas après avoir pris acte du résultat défavorable de l'expertise ce qui serait contraire à la bonne foi – à la direction de la procédure[476].

457 Une fois saisie d'une annonce ou d'une demande de récusation, la direction de la procédure rend une décision. Dans les cas définis à l'art. 56 let. b à e CPP, la vérification est en principe évidente et ne nécessite pas de formalités supplémentaires (art. 59 al. 1 *a contrario* CPP), la simple déclaration du motif suffit à destituer l'expert. Au contraire, une décision formelle motivée par écrit (art. 59 al. 1 let. a à d CPP) est nécessaire lorsque le motif de récusation s'appuie sur l'art. 56 let. a ou f CPP. L'autorité admet la récusation en se basant sur l'avis ou sur la requête sans nécessairement entreprendre des mesures probatoires supplémentaires si les motifs sont suffisants et, si tel n'est pas le cas, elle cherche à déterminer si le motif allégué est justifié ou non *in casu*. En outre, en cas d'opposition de l'expert à sa récusation, une décision formelle doit toujours être prise[477] dans le dessein d'assurer le droit à la motivation des décisions.

458 En sus de la récusation, la mission de l'expert peut s'interrompre suite à la révocation du mandat par la direction de la procédure. Cette possibilité octroyée aux autorités pénales doit servir l'intérêt de la cause à juger, notamment lorsque des doutes grandissant quant à un motif de récusation absolu intervient, lorsque la mission se précise et va au-delà des

[474] ATF 122 IV 235, 237-239 = JdT 1998 IV 119, 119-121; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 283; SCHMID, Handbuch, p. 388.

[475] HAUSER, SCHWERI, HARTMANN, p. 120; Polizeiliche Ermittlung-VOSER, p. 82-83.

[476] ATF 119 Ia 221, 227-229 = JdT 1994 IV 190; ATF 128 V 82, 85-86; ATF 132 II 485, 496-497; ATF 134 I 20, 21-22; HAUSER, SCHWERI, HARTMANN, p. 119; KAUFMANN, p. 163; PERRIER DEPEURSINGE, art. 58, p. 75.

[477] Polizeiliche Ermittlung-VOSER, p. 85.

connaissances professionnelles du spécialiste[478] ou lorsqu'il y a négligence de la part de l'expert (art. 191 CPP).

b. Les conséquences de la récusation et de la révocation

459 Le mandat accréditant la tâche de l'expert désigné n'a pas un caractère définitif et irrévocable. En cas d'acceptation de la récusation ou de révocation, soit l'expert n'entre pas en fonction soit il est destitué et doit cesser sa mission immédiatement. Dans cette seconde circonstance, hormis si la récusation intervient pour négligence (art. 191 let. b CPP) – non-respect des délais ou des obligations –, l'expert reçoit une indemnité pour le dédommager du travail déjà fourni (art. 190 CPP)[479].

460 L'expertise qui a déjà débuté n'est pas nulle de plein droit. Le rapport écrit est en principe écarté du dossier[480], mais le nouvel expert peut continuer l'expertise en se basant sur les travaux du spécialiste récusé. Cependant, la partie qui demande la récusation peut conclure à l'annulation des actes de procédure déjà réalisés nécessitant la répétition de l'expertise (art. 60 al. 1 CPP), exception faite des mesures probatoires non-renouvelables qui peuvent être prises en considération (art. 60 al. 2 CPP). Un délai de seulement cinq jours suivant la connaissance du motif de récusation est prévu pour demander la répétition des actes (art. 60 al. 1 CPP). Andreas Donatsch et Claudine Cavegn estiment cette mesure d'annulation insatisfaisante[481]. Nous sommes du même avis. L'obligation qui est faite à la partie désirant se prévaloir d'un motif d'annulation et de répétition dans un délai de cinq jours nuit à la bonne administration de la justice et à la confiance des parties envers l'expert. Il ne faut pas perdre de vue que ce dernier est désigné exclusivement par la direction de la procédure et que les parties doivent pouvoir s'y fier. Il est donc essentiel qu'elles puissent demander l'annulation et la répétition des actes en cas de besoin. A notre sens, il est recommandé au plaideur de déposer sa demande de récusation dans les cinq jours accompagnée d'une demande d'annulation en cas de besoin. Lors d'un prononcé d'une révocation pour motif impérieux, la crédibilité de l'expertise incomplète étant largement amoindrie, il serait préférable d'aller plus loin en prévoyant la répétition de l'expertise d'office.

---

[478] BSK-StPO-HEER, art. 184 N 33; SCHMID, Handbuch, p. 386.

[479] Message, CPP, 1193.

[480] CR-CPP-VERNIORY, art. 60 N 1; CR-CPP-VUILLE, art. 183 N 31; StPO-KELLER, art. 60 N 3.

[481] DONATSCH, CAVEGN, RPS 2008, p. 171; DONATSCH, CAVEGN, SJZ 2007, p. 410.

461 Au surplus, qu'il s'agisse d'une récusation ou révocation au sens des art. 56 ss, 183 al. 3, 184 al. 5 ou 191 let. b CPP, la conséquence est identique puisqu'elle engendre la nomination d'un nouvel expert.

C. Le déroulement de l'expertise

1. La communication de la mission et l'obligation d'accepter

462 L'expertise commence avec l'instruction de l'expert comportant deux volets: la communication de la mission et les consignes relatives à la bonne exécution de l'expertise.

463 Généralement, le mandat rédigé contenant les questions, les obligations et la conséquence de leur violation – l'attention de l'expert est notamment attirée sur les conséquences d'une fausse expertise (art. 307 CP) ou de la violation du secret professionnel (art. 320 CP) – est remis à l'expert qui en prend acte avant de débuter ses démarches. Exceptionnellement, en cas d'urgence – par exemple, si le technicien est désigné durant le transport sur place –, la communication de l'expertise se fait oralement et est consignée ultérieurement au procès-verbal. Outre pour éviter tout retard dans la procédure, la forme verbale à l'avantage d'expliciter de manière concrète les problématiques à résoudre[482], de faciliter l'échange entre l'expert et l'autorité judiciaire et de permettre à l'expert l'émission d'observations, suggestions ou interrogations sans devoir surseoir à l'exécution de l'expertise.

464 Auparavant, certains cantons[483] prévoyaient explicitement l'interdiction pour l'expert compétant de décliner la mission. D'autres législations cantonales niaient simplement la possibilité d'accepter ou de refuser la tâche, alors que certaines procédures pénales cantonales instauraient l'obligation pour l'expert de prêter serment, d'accomplir la mission conférée ou de promettre de l'exécuter dans les règles de l'art et de la conscience. La Commission d'expert "Unification de la procédure pénale" a renoncé à codifier expressément l'obligation d'accepter la mission[484]. Niklaus Schmid et Daniel Jositsch spécifient qu'avant l'établissement du mandat, l'expert est libre de renoncer à la mission si aucune obligation professionnelle ne le force à accepter[485]. A défaut d'une disposition dans le CPP similaire à l'art. 89 PPM, il n'existe donc aucun devoir général de réaliser l'expertise.

---

[482] KAUFMANN, p. 169-170.

[483] art. 130 al. 1 aCPP/BE; art. 92 al. 1 aCPP/FR; art. 68 aCPP/GE; art. 173 al. 1 aCPP/JU; art. 157 al. 1 aCPP/NE; art. 105 ch. 2 et 106 aCPP/VS.

[484] De 29 à l'unité, p. 107.

[485] JOSITSCH, Strafprozessrechts, p. 109; SCHMID, Handbuch, p. 386-387.

465 Ces deux doctrines n'éclaircissent cependant pas la problématique à partir du moment où l'expert est désigné par une décision. En l'absence d'une norme instaurant le droit de refuser la mission, il faut en conclure que le mandat est de nature impérative. Une fois la mission assignée – sauf inaptitude de l'expert (art. 183 al. 1 *a contrario* CPP) ou raison légitime (183 al. 3 CPP *cum* 56 ss CPP, voire 184 al. 5 CPP) –, l'expert désigné a l'obligation d'accepter la mission qui lui est confiée et de l'exécuter de manière consciencieuse.

2. L'exécution de l'expertise

466 En droit suisse, le système de l'expert officiel a prévalu sur le système de la *common law*[486] impliquant que l'expertise n'est pas contradictoire dès lors que l'avis des parties sur la désignation du spécialiste et de sa mission n'est pas contraignant. En contrepartie du caractère non contradictoire de l'expertise, l'expert est tenu strictement à la bonne exécution de sa charge en respectant les obligations qu'il a envers la direction de la procédure et en justifiant ses travaux.

467 L'expert nommément désigné répond en principe personnellement de sa mission (art. 185 al. 1 CPP) et est seul responsable de son exécution. Lorsqu'avec l'accord de la direction de la procédure (art. 184 al. 2 let. b CPP) le spécialiste fait appel à un ou des collaborateurs ou autres experts agissant sous ses ordres, il engage sa propre responsabilité pour les actes de ces tiers[487]. En revanche, si l'expert sollicite l'éclaircissement d'une question échappant à sa spécialité, la direction de la procédure mandate un nouvel expert ou expert-adjoint[488] en charge d'élucider le point problématique qui n'engage pas la responsabilité du premier.

468 Dans le dessein de permettre une exécution adéquate, les rapports entre la direction de la procédure et l'expert sont transparents[489]. Les circonstances de l'affaire ou toutes informations sur celle-ci sont fournies au spécialiste. En outre, la direction de la procédure met à disposition de l'expert tous les documents provenant du dossier de procédure et considérés, par elle, comme importants pour l'établissement de l'expertise (art. 184 al. 4 CPP)[490].

---

[486] LECLERC O., p. 174-175.

[487] CR-CPP-VUILLE, art. 185 N 17; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 179; MOREILLON, PAREIN-REYMOND, art. 184 N 10-11; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 286; StPO-DONATSCH, art. 184 N 17.

[488] MOREILLON, PAREIN-REYMOND, art. 184 N 13; PIQUEREZ, Traité de procédure pénale suisse, p. 389; SCHMID, Praxiskommentar, art. 184 N 6-7 ; StPO-DONATSCH, art. 184 N 18.

[489] BSK-StPO-HEER, art. 184 N 16-17; CR-CPP-VUILLE, art. 184 N 28.

[490] BSK-StPO-HEER, art. 184 N 28 ss; CPP-Commentario-GALLIANI, MARCELLINI, art. 185 N 5; KAUFMANN, p. 170.

469 En tant qu'auxiliaire, en principe, l'expert ne peut pas entreprendre des actes d'instruction. Cette restriction doit être relativisée, puisque le professionnel peut être autorisé par la direction de la procédure à poser des questions aux témoins et aux parties en se limitant aux éléments essentiels – d'ordre technique – pour accomplir son expertise (art. 185 al. 2 CPP). Il a également la possibilité d'obtenir des compléments en ajoutant au dossier de procédure des documents disponibles, mais non fournis, ou en requérant à d'autres mesures probatoires[491] (art. 185 al. 3 CPP).

470 Dans l'hypothèse où les documents fournis ne sont pas suffisants pour établir le rapport d'expertise, l'autorité judiciaire peut autoriser l'expert à entreprendre de simples investigations (art. 185 al. 4 CPP) – si elles sont prévisibles, l'autorisation fait partie intégrante du mandat; sinon l'octroi de l'autorisation intervient en cours de procédure après sollicitation[492] –, notamment en entreprenant des visites du lieu de l'infraction pour récolter des renseignements supplémentaires, réaliser des examens médicaux sur les personnes impliquées ou suspectées, voire recourir à certains documents additionnels. Toutefois, il ne peut procéder qu'aux investigations qui relèvent de sa spécialité et qui sont indispensables à l'exécution du mandat[493] sans élucider l'ensemble de l'affaire de sa propre initiative. Lorsque l'expert fait usage de cette possibilité, les personnes convoquées ont le droit de refuser de répondre à la convocation, mais peuvent être amenées par la police (art. 185 al. 5 *in fine* CPP). Il appartient en outre à l'expert d'informer le prévenu et les personnes en droit de refuser de déposer ou de témoigner au début de l'investigation de ce droit (art. 185 al. 5 CPP) sans quoi l'acte peut être invalidé et donc inexploitable (art. 177 al. 2 CPP par analogie et 141 al. 2 CPP). L'expert étant un scientifique ou un technicien et non pas un juriste, cette obligation n'est pas sans créer des difficultés dans son application.

3. La participation des parties à l'expertise

471 Les parties ont généralement le droit de participer à l'administration des preuves (art. 147 al. 1 CPP). La Cour européenne des droits de l'homme a rappelé qu'une procédure équitable (art. 6 § 1 CEDH, art. 14 § 1 Pacte II et art. 29 al. 1 Cst) comporte l'élément de caractère contradictoire donnant la faculté aux parties de connaître les éléments nécessaires au succès de leurs prétentions, de connaître et discuter les pièces du dossier. De ce principe, la Cour de

---

[491] Message, CPP, p. 1193; MOREILLON, PAREIN-REYMOND, art. 184 N 13; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 286-287; RIEDO, FIOLKA, NIGGLI, p. 211; SCHMID, Praxiskommentar, art. 185 N 5.

[492] Message, CPP, p. 1193; RUCKSTUHL, DITTMANN, ARNOLD, p. 174.

[493] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 166; KAUFMANN, p. 170; Message, CPP, p. 1193; RIEDO, FIOLKA, NIGGLI, p. 211; StPO-DONATSCH, art. 185 N 4.

Strasbourg a conclu que les parties sont en droit d'assister aux entretiens conduits par un expert ou de recevoir les pièces prises en compte par celui-ci[494]. Toutefois, ce droit n'est pas absolu puisque le principe de contradiction doit être respecté *in globo*, soit dans son entier et non par phase.

472 Lors des travaux parlementaires, la participation des parties à l'exécution de l'expertise a été rejetée[495].

473 Ce rejet semble quelque peu radical. L'expertise a une importance considérable en procédure pénale, notamment quant à la force probante qui lui est accordée[496]. Certes, les parties ont le droit de se prononcer sur la mission de l'expert, de l'interroger ou de produire des expertises privées afin de respecter le principe de contradiction. Néanmoins, dans certaines situations exceptionnelles où l'expertise prendrait une place prépondérante dans la décision judiciaire, il paraît être adéquat que les parties puissent participer à son processus d'élaboration de manière plus étendue. Nous préconisons par exemple que l'expert tienne à disposition des parties les documents de travail, ce qui leur permettrait d'avoir un droit de regard *a posteriori*.

474 Ainsi, l'exclusion de principe des parties au processus d'expertise doit rester la règle pour garantir l'indépendance de l'expert, mais ne doit pas être systématique ou absolue.

4. La rédaction et le dépôt du rapport d'expertise

475 Une fois l'expertise établie et dans le délai imparti par la direction de la procédure, l'expert dépose son rapport, en principe sous la forme écrite, pour relater les travaux entrepris et formuler les conclusions auxquelles il a abouti (art. 187 al. 1 CPP). L'écrit implique l'obligation que le ou les expert(s) désigné(s) dans le mandat – et nul autre, le droit de signature n'étant pas transmissible – appose(nt) leur signature sur le rapport d'expertise[497]. Dans certains cas, notamment si les premiers éléments doivent être récoltés rapidement, l'autorité judiciaire compétente peut ordonner que l'expertise soit délivrée oralement ou qu'un rapport écrit soit commenté, voire complété oralement (art. 187 al. 2 CPP). Dans ces

[494] CourEDH, Affaire *Lobo Machado c. Portugal*, arrêt du 20 février 1996, 15764/89, § 31; CourEDH, Affaire *Mantovanelli c. France*, arrêt du 18 mars 1997, 21497/93, § 33-34; CourEDH, Affaire *Oral c. Turquie*, arrêt du 25 novembre 2008, 18384/04, § 30.

[495] SCHMID, Praxiskommentar, art. 185 N 10.

[496] Infra Partie II, Chapitre 1, III, C, n° 497 ss.

[497] BSK-StPO-HEER, art. 187 N 1; CPP-Commentario-GALLIANI, MARCELLINI, art. 187 N 1; MOREILLON, PAREIN-REYMOND, art. 184 N 2; SCHMID, Praxiskommentar, art. 187 N 1.

circonstances, les dispositions sur l'audition des témoins sont applicables comprenant notamment le droit de refuser de témoigner (art. 168 ss CPP), l'exhortation à déposer conformément à la vérité sous peine de faux témoignage (art. 307 CP) et l'obligation pour l'autorité de vérifier les liens relationnels pouvant exister avec les parties (art. 177 al. 2 CPP)[498].

476 En revanche, à notre sens, l'expert est en droit de bénéficier d'une copie de son procès-verbal contrairement au témoin dès lors que son audition orale constitue un complément d'expertise. Ainsi, les déclarations orales de l'expert sont une alternative à l'écrit qui a la même finalité soit de recueillir un avis complémentaire. C'est pourquoi l'expert n'est pas un véritable témoin et peut avoir accès à son procès-verbal d'audition.

477 Quant au contenu du rapport et des conclusions d'expertise, il n'est pas réglementé, mais un accord d'ordre général existe. Ainsi, le langage utilisé dans l'expertise doit être clair, précis et compréhensible pour les juges et pour les parties. L'expertise doit comprendre un récapitulatif des conditions de mise en œuvre avec la désignation de l'expert, le contenu du mandat et le libellé des questions à éclaircir ainsi qu'un résumé des faits analysés, des travaux entrepris, des problématiques rencontrées, les discussions ayant eu lieu, les conclusions prises répondant à la totalité des questions et uniquement à celles-ci, voire des incidences en cas de manquement/lacune sur une question[499].

478 Dès le dépôt du rapport d'expertise, la phase des débats débute. Grâce à la facilité d'accès du dossier d'expertise, à sa complétude et à sa clarté, les parties – principalement le prévenu ainsi que ses représentants – peuvent aisément s'y référer pour formuler leurs observations (art. 188 CPP) et, grâce à la transparence, faire valoir leur droit d'être entendus[500]. Au besoin, un complément d'expertise ou une clarification peut être demandé. En outre, le synchronisme des points devant être contenus dans le rapport permet le contrôle de la bonne marche des opérations réalisées par le technicien (art. 189 CPP)[501].

---

[498] Message, CPP, p. 1194.

[499] BÜHLER, p. 572-573; CPP-Commentario-GALLIANI, MARCELLINI, art. 187 N 2; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 179; PIQUEREZ, Traité de procédure pénale suisse, p. 389; Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 289; SCHMID, Praxiskommentar, art. 187 N 3; WIPRÄCHTIGER, p. 209.

[500] KAUFMANN, p. 171-172; MOREILLON, PAREIN-REYMOND, art. 188 N 2; SCHMID, Praxiskommentar, art. 188 N 1.

[501] JOSITSCH, Strafprozessrechts, p. 111; KAUFMANN, p. 171; SCHMID, Handbuch, p. 394.

III. L'appréciation et la valeur probante de l'expertise

A. Le contrôle du juge et des parties

479 Les preuves administrées durant le procès étant promptes à fonder une décision de culpabilité, la Cour européenne des droits de l'homme a insisté sur l'importance de l'administration de la preuve et de la nécessité de respecter l'égalité des armes entre la défense et l'accusation[502]. La phase de désignation de l'expert et d'établissement de l'expertise étant non-contradictoire, l'équité exige en particulier que la défense puisse contrôler postérieurement les travaux entrepris. Tout moyen de preuve doit être soumis au débat contradictoire permettant au prévenu ou à son représentant de faire valoir leurs observations et de contester la crédibilité d'une preuve. L'expertise judiciaire n'est pas épargnée par le principe de contradiction[503].

480 L'autorité judiciaire doit pouvoir soumettre à son libre arbitre le contenu de l'expertise pour motiver sa décision. N'ayant pas les aptitudes professionnelles, il est nécessaire que la crédibilité des conclusions soit certaine et intelligible. Afin de respecter l'équité des débats[504] et le droit d'être entendu[505], le juge communique aux parties les écrits du spécialiste avec un délai pour formuler leurs observations. Ainsi, le rapport d'expertise est soumis au contrôle du magistrat et des parties.

481 En d'autres termes, le juge et les parties vérifient si les conclusions sont complètes, compréhensibles et exactes[506].

482 Les conclusions sont signalées comme complètes, si les connaissances professionnelles et les faits ayant servis à appuyer l'avis du spécialiste sont intégralement exposés et que toutes les questions libellées trouvent une réponse. *A contrario*, est incomplet le rapport qui ne contient

---

[502] CourEDH, Affaire *Van Mechelen et autres c. Pays-Bas*, arrêt du 23 avril 1997, 21363/93, 21364/93, 21427/93 et 22056/93, § 50-55; CourEDH, Affaire *Augusto c. France*, arrêt du 11 janvier 2007, 71665/01, § 50; CourEDH, Affaire *McKeown c. Royaume-Uni*, arrêt du 11 janvier 2011, 6684/05, § 43.

[503] CourEDH, Affaire *Mantovanelli c. France*, arrêt du 18 mars 1997, 21497/93, § 33; CourEDH, Affaire *G.B c. France*, arrêt du 02 octobre 2001, 44069/98, § 69-70; CourEDH, Affaire *Augusto c. France*, arrêt du 11 janvier 2007, 71665/01, § 50.

[504] ATF 118 Ia 144, 145-146; ATF 127 I 73, 81-82.

[505] BSK-StPO-HEER, art. 187 N 10 et art. 189 N 1; CPP-Commentario-GALLIANI, MARCELLINI, art. 188 N 1; JOSITSCH, Strafprozessrechts, p. 111; PIQUEREZ, Traité de procédure pénale suisse, p. 389; SCHMID, Handbuch, p. 394.

[506] BSK-StPO-HEER, art. 189 N 1 ss; BÜHLER, p. 573; DONATSCH, Jusletter, n° 47; HAUSER, SCHWERI, HARTMANN, p. 314; RIKLIN, Strafprozessordnung, art. 189 N 1-2; WIPRÄCHTIGER, p. 207.

pas toutes les données utiles[507]. Ne pouvant s'appuyer sur des imprécisions sans violer la présomption d'innocence, le magistrat procède alors à l'obtention des compléments utiles (art. 189 let. a CPP).

483 Les conclusions sont compréhensibles, si les éléments rattachés à l'expertise et leurs conséquences sont à la portée de la direction de la procédure et des parties. La justice saisissant un technicien pour l'aider dans sa tâche, des explications peu claires sont inutiles raison pour laquelle l'expert privilégie l'usage d'un langage simple plutôt que technique et précise au mieux comment ses conclusions se sont forgées.

484 Pour terminer, les conclusions sont convaincantes si elles sont concordantes avec les avis doctrinaux et la logique. La vérification de la réalisation de cette condition est la plus ardue. L'avis de l'expert ne doit pas être écarté ou clarifié uniquement parce qu'une autre doctrine expose l'opinion inverse. En conséquence, si l'expert, par ses connaissances professionnelles, constate un différend scientifique, il explique sa position et spécifie pourquoi il choisit telle doctrine plutôt qu'une autre afin d'éviter toute contradiction non-justifiée.

485 Dans la mesure où il serait arbitraire de considérer les faits comme prouvés si le rapport est incomplet, imprécis ou inexact, la justice procède d'office à l'examen du rapport d'expertise. Elle vérifie si l'expert a répondu aux questions libellées dans le mandat, sans quoi des informations supplémentaires doivent être obtenues, et détermine si de nouvelles questions s'imposent[508].

486 Les parties ou leurs avocats s'appuyant sur les mêmes écrits peuvent émettre le souhait de soumettre des questions additionnelles à l'expert. Généralement, le droit d'interagir intervient parce que la défense et l'accusation ont un parti pris en souhaitant que les conclusions leur soient favorables. Elles vont donc tenter d'introduire des doctrines divergentes ou de modifier l'avis de l'expert à l'aide de nouvelles questions[509].

487 En outre, lorsque les faits à l'appui de l'expertise ou les résultats de l'expert paraissent incomplets (art. 189 let. a CPP) ou incorrects (art. 189 let. b et c CPP), une demande, d'office ou sur réquisition d'une partie, est émise pour combler les lacunes par des renseignements complémentaires (art. 189 hyp. 1 et 2 CPP). Si des questions complémentaires ou explicatives ne sont pas suffisantes, l'autorité compétente désigne un nouvel expert (art. 189 hyp. 3 CPP) pour formuler une contre-expertise. De plus, la lecture du rapport apportant des

[507] CR-CPP-VUILLE, art. 189 N 8-10; DONATSCH, Jusletter, n° 45; KAUFMANN, p. 220.

[508] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 180; KAUFMANN, p. 173-174.

[509] KAUFMANN, p. 175-176.

connaissances approfondies au juge ou au ministère public, il est possible que des faits supplémentaires inconnus soient constatés grâce au rapport d'expertise et doivent être élucidés à leur tour. Ces conséquences valent de même lorsque la direction de la procédure fait appel à plusieurs experts et qu'ils n'arrivent pas aux mêmes conclusions (art. 189 let. b CPP)[510].

488 Plus complexe est la résolution de la problématique liée à un état de fait technique. Le non-expert ne peut que difficilement s'assurer de la logique et de l'exactitude de connaissances techniques ou scientifiques qu'il ne maîtrise pas. Face à une telle situation, il est admissible, en cas de probable cohérence dans le dossier, de faire confiance à l'expert et de renier tout doute[511].

489 Les vérifications concernant les exigences sur le contenu de l'expertise, l'écoulement du délai imparti aux parties pour formuler leurs observations et l'apport d'éventuelles clarifications ou compléments clôturent la phase des débats contradictoires sur l'expertise judiciaire. Exception faite des cas où un nouvel expert doit être désigné et une nouvelle expertise établie[512], le rapport est reconnu comme un moyen de preuve fiable. Il peut être soumis à la libre appréciation du juge du fond[513].

B. L'appréciation du rapport d'expertise

1. La direction de la procédure connaît le droit

490 En vertu du principe *iura novit curia*, la direction de la procédure connaît le droit et n'est donc pas tenue à l'argumentation juridique des parties. L'expertise, considérée comme un moyen de preuve, sert à établir uniquement les faits. Néanmoins, il est parfois délicat de distinguer le fait du droit.

491 Pour illustrer la problématique, prenons le cas d'un dommage à la propriété causé par une personne atteinte d'une maladie mentale. Le juge demande à un expert médical d'évaluer l'incapacité de l'auteur pour déterminer s'il s'agit d'un cas d'irresponsabilité (19 al. 1 CP) ou

---

[510] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-SOLLBERGER, p. 180; MAURER, p. 231; MOREILLON, PAREIN-REYMOND, art. 189 N 1-3.

[511] Par analogie entre le CPC et le CPP: KAUFMANN, p. 221.

[512] A ce sujet: TF 6B_283/2007 du 5 octobre 2007, c. 2; WIPRÄCHTIGER, p. 212.

[513] JOSITSCH, Strafprozessrechts, p. 111; PERRIER DEPEURSINGE, art. 189, p. 238; SCHMID, Handbuch, p. 395; SCHMID, Praxiskommentar, art. 189 N 2.

de responsabilité restreinte (art. 19 al. 2 CP). L'évaluation doit se baser uniquement sur un élément de fait et de manière abstraite, afin de déterminer si l'auteur est faible d'esprit ou est atteint d'un trouble mental grave.

492 Le tribunal doit s'assurer que la question qui est posée à l'expert se limite à l'état de fait et n'est pas sujette à une réponse sur le droit, à savoir si l'auteur est en état d'irresponsabilité ou de responsabilité restreinte. Il est néanmoins possible que le juge pose clairement une question de fait et que l'expert fournisse une réponse avec un avis juridique. Dans une telle hypothèse, le magistrat doit se limiter à apprécier l'état de fait établi ou prouvé par l'expertise.

493 Il est impératif que le juge ne se décharge pas de sa mission en administrant une preuve et en ratifiant l'avis juridique de l'expert sans l'apprécier[514]. Ce constat vaut de même lorsque le ministère public recourt à une expertise. Selon le principe *iura novit curia*, la direction de la procédure doit donc éviter de poser des questions demandant une réponse juridique et/ou de tenir compte de l'avis juridique de l'expert. Elle doit s'en tenir à l'établissement des faits par l'expertise comme moyen de preuve et apprécier ce qui est démontré.

2. L'évaluation des faits allégués

494 Théoriquement, n'ayant aucune force spéciale comme tous les autres moyens de preuves, l'avis de l'expert ne lie pas le juge. "*Les juges restent les appréciateurs souverains des faits comme des résultats de l'expertise: ils doivent se prononcer sur tous les points qui sont affirmés par l'expert, d'après leur intime conviction.*"[515]. Le rapport d'expertise constitue un simple renseignement dont la justice répressive tire des conséquences après l'avoir apprécié (art. 10 al. 2 CPP)[516].

495 Il incombe au juge d'estimer la crédibilité des raisonnements de l'expert, la pertinence des conclusions et leurs conséquences à la lumière de l'état de fait à juger. Pour ce faire, il s'appuie notamment sur la cohérence du rapport et l'absence de contradiction, la logique du raisonnement ou encore la concordance du rapport avec l'avis doctrinal majoritaire[517]. Une fois reconnu, l'avis de l'expert est considéré comme exact et convaincant. Toutefois, cette

[514] ATF 118 Ia 144, 145-146; ATF 127 I 73, 81-82; ATF 135 III 670, 677.

[515] GARRAUD, T. I, p. 631.

[516] ATF 96 IV 97, 98; ATF 129 I 49, 57-58 = JdT 2005 IV 141, 148-149; 136 IV 55, 61 = JdT 2010 IV 127, 132-133.

[517] BÜHLER, p. 573; CR-CPP-VUILLE, art. 182 N 9; PIQUEREZ, Traité de procédure pénale suisse, p. 390; WIPRÄCHTIGER, p. 207.

tâche est particulièrement ardue pour le juge du fond qui recourt justement au spécialiste pour lui fournir les explications qu'il ignore.

496 Ainsi, la nécessité d'avoir l'intime conviction implique que le magistrat peut – en énonçant les motifs le justifiant – s'écarter en totalité ou en partie de l'avis de l'expert[518]. Cependant, l'expérience démontre que ce postulat est purement théorique au vu de la difficulté, pour un juriste, d'appréhender les considérants scientifiques et techniques[519].

C. La valeur probante du rapport d'expertise

1. La difficulté pour le juge de s'écarter du rapport d'expertise

497 L'expertise judiciaire apparaît comme un moyen adéquat de découvrir la vérité matérielle en découvrant et/ou en appréciant une preuve ou un indice.

498 La raison qui fonde l'appel à un spécialiste et l'axiome théorique sur l'absence d'autorité du rapport d'expertise ne se situe pas dans une logique sans faille. Il est en effet paradoxal de recourir à un expert par manque de compétence et de pouvoir, lors de la formation de l'intime conviction, dénier la fiabilité d'un rapport d'expertise fondé justement sur les aptitudes professionnelles du spécialiste[520]. D'autant plus que le juge souhaitant s'écarter des conclusions de l'expert doit le justifier alors même qu'il n'a pas les connaissances spéciales permettant de contrer l'avis éclairant l'état de fait technique ou scientifique. Sur le plan intellectuel, il est inconcevable de réfuter les résultats de l'expertise alors que leur contenu échappe clairement à la faculté d'examen du juge. C'est pourquoi, en réalité, l'expertise a une valeur accrue dont le juge ne peut s'éloigner qu'en cas de justes motifs difficilement réunis[521].

499 En toute logique, si des faits ou indices cruciaux font naître un doute sur la crédibilité du rapport d'expertise, le juge doit réfuter la valeur probante de cette preuve. En effet, en se fondant sur une expertise non concluante – notamment parce qu'elle contient des informations contradictoires, lacunaires ou erronées, ou lorsque l'opinion de l'expert est

[518] ATF 55 II 225, 226 = JdT 1930 I 98,100; ATF 81 II 259, 263 = JdT 1956 I 291, 293; ATF 87 I 87, 90; ATF 101 IV 129, 130 = JdT 1976 IV 42, 44-45; ATF 118 Ia 144, 146-147; ATF 129 I 49, 57-58 = JdT 2005 IV 141, 148-149; ATF 136 IV 55, 61 = JdT 2010 IV 127, 132-133; TF 1B_325/2013 du 11 octobre 2013, c. 4.2; ; CR-CPP-VUILLE, art. 182 N 7; JEANNERET, KÜHN, p. 242; JOSITSCH, Strafprozessrechts, p. 111; PERRIER DEPEURSINGE, art. 189, p. 238; SCHMID, Handbuch, p. 395; SCHMID, Praxiskommentar, art. 189 N 2.

[519] Infra Partie II, Chapitre 1, III, C, 1, n° 497 ss.

[520] ANTOGNINI, p. 7; BOURCIER, DE BONIS, p. 89-90; DONATSCH, CAVEGN, SJZ 2007, p. 410; RASSAT, p. 437.

[521] ATF 118 Ia 144, 145-146; ATF 125 V 351, 352-353; ATF 127 I 73, 81-82; ATF 129 I 49, 57-58.

indéfendable ou encore parce qu'après désignation, il s'avère que l'expert n'a pas les connaissances requises[522] –, le juge apprécie arbitrairement une preuve et viole l'art. 9 Cst[523].

500 Au surplus, la libre appréciation du juge (art. 10 al. 2 CPP) ne doit pas être un prétexte pour que le magistrat se constitue comme expert en s'écartant délibérément des conclusions du technicien: "[...] *nul ne peut être à la fois juge et expert.*"[524]. Sous peine d'arbitraire, le magistrat désirant s'écarter de l'expertise doit motiver sa décision.

501 De plus, étant plus apte, par la procédure de certification qui l'accrédite (183 CPP)[525], à être impartial qu'un témoin, un présumé coupable, une victime ou une personne appelée à donner des renseignements, les experts ont – pour l'opinion publique et la justice – plus de crédit puisqu'ils fournissent un avis scientifique reposant sur des bases solides de la technique ou de la science facilement démontrables. C'est d'ailleurs pour cela que l'expert est considéré comme un auxiliaire du juge et non comme un simple témoin impliquant que son avis n'est pas sans importance. Généralement, l'objectivité des sciences ou techniques et les difficultés liées à la motivation de l'avis divergeant du juge ou à la constatation de problèmes entachant l'expertise rendent difficile l'écartement des conclusions de l'expert. Ainsi, les magistrats sont souvent amenés à s'inspirer largement de l'avis de l'expert contrairement à ce qu'ils sont amenés à faire avec les dires d'autres participants à la procédure.

502 En définitive, l'absence de formation des juristes et le manque de communication directe[526] avec l'expert restreignent grandement les débats sur les moyens de preuves scientifiques et le développement relatif à l'interprétation des données. Face à cette situation d'absence d'aptitude technique, les juges du fond sont tentés d'accorder leur confiance aveugle aux résultats fournis par l'expert et à l'évaluation limitée qu'ils peuvent en faire[527]. Ces affirmations nous forcent à constater que le poids du rapport d'expertise dans l'appréciation des preuves se renforce. En effet, appréhendant plus aisément les réponses basiques, une tendance marquée à privilégier uniquement les conclusions de l'expertise se dessine impliquant que les magistrats se rallient presque unanimement aux réponses fournies.

---

[522] ATF 55 II 225, 226 = JdT 1930 I 98, 100; ATF 81 II 259, 263 = JdT 1956 I 291, 293-294; ATF 87 I 87, 90; ATF 101 IV 129, 130 = JdT 1976 IV 42, 44-45; ATF 118 Ia 144, 145-146; ATF 128 I 81, 86; ATF 136 II 539, 547-548.

[523] ATF 118 Ia 144, 146; ATF 127 I 73, 81-82; ATF 136 IV 539, 547-548; TF 1B_325/2013 du 11 octobre 2013, c. 4.2; DONATSCH, Jusletter, n° 47; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 167; MOREILLON, PAREIN-REYMOND, Intro art. 182 ss N 8; PERRIER DEPEURSINGE, art. 189, p. 238.

[524] MERLE ET VITU, T. II, p. 273, n. 4 *in fine*.

[525] Polizeiliche Ermittlung-ARMBRUSTER, VERGERES, p. 280; VUILLE, Thèse, p. 358-360.

[526] OBERHOLZER, Strafprozessrechts, p. 301-302; WIPRÄCHTIGER, p. 213 et 215 ss.

[527] MANGIN, TARONI, p. 510; PIQUEREZ, Traité de procédure pénale suisse, p. 390-391; RASSAT, p. 437.

503 L'expertise a donc une valeur probatoire supérieure aux autres preuves, dont le juge se distancie uniquement pour des raisons infaillibles et motivées[528]. Cette constatation nous mène à nous interroger sur les conséquences du recours à l'expertise envers les principes généraux du droit de la preuve et de l'ingérence de l'expert dans la procédure pénale, plus précisément dans la mission du magistrat.

504 En vertu de la procédure pénale mixte, des droits fondamentaux et du système de la preuve morale, le juge décideur doit être indépendant et juger selon son intime conviction. Le principe d'indépendance veut que le magistrat répressif ne puisse pas être influencé par une cause extérieure. Ainsi, il ne peut pas être lié au pouvoir exécutif ou législatif et sa conduite ne peut pas être dictée totalement ou partiellement par une autre personne. De plus, sa décision doit reposer sur son intime conviction signifiant qu'il rend un jugement en son âme et conscience. En exigeant de la justice d'avoir des raisons techniques suffisantes pour rejeter les conclusions de l'expertise et en reconnaissant plus de crédibilité à l'avis scientifique qu'à la déclaration du témoin, une limite implicite est fixée à l'intime conviction réduisant l'indépendance du juge. Premièrement, le juge n'est plus libre d'apprécier selon ses croyances les preuves, corrélativement la valeur probatoire, du rapport d'expertise. Deuxièmement, l'expert – même s'il n'est qu'un auxiliaire du juge et ne doit pas répondre à des questions de droit – peut avoir une large influence sur la décision de culpabilité, puisqu'il connaît les difficultés pour un juge de réfuter les conclusions techniques déposées.

505 Par conséquent, il n'est pas erroné d'affirmer qu'avec l'évolution de la science et des techniques, la procédure pénale se modifie. De la preuve purement morale, nous apercevons la naissance des preuves scientifiques. Pour appréhender et comprendre correctement ces moyens probatoires, l'appel à un spécialiste est l'unique solution entrevue jusqu'alors. Avec le progrès exponentiel dans le domaine des nouvelles technologies, l'expert va devenir un acteur indispensable de la procédure judiciaire. Le risque est donc de voir l'intime conviction du juge se fonder de plus en plus sur la conscience et les connaissances d'une autre personne que lui-même. Si tel est le cas, le principe de l'intime conviction et, avec lui, le système de justice sont mis en péril; le juge ne pourra plus juger sans l'avis d'un expert, alors même que ce dernier n'a pas toujours conscience des conséquences juridiques de ses affirmations et – surtout – n'a pas l'aptitude pour influencer les questions de droit.

506 Aujourd'hui, certains praticiens ou théoriciens du droit proposent de former les magistrats. Cette solution doit permettre d'éviter le recours systématique à un expert ou de réfuter plus aisément ses conclusions, voire que le magistrat puisse instruire, contrôler et superviser

[528] CPP-Commentario-GALLIANI, MARCELLINI, art. 189 N 6; CR-CPP-VUILLE, art. 182 N 10; DONATSCH, Jusletter, n° 49; JOSITSCH, Strafprozessrechts, p. 111; PERRIER DEPEURSINGE, art. 189, p. 238; SCHMID, Handbuch, p. 395.

l'expertise[529]. L'aboutissement de l'exégèse des neuf moyens de preuves scientifiques ou technologiques affirmera ou infirmera la pertinence de cette proposition[530].

2. L'évaluation de l'incertitude

507 Outre la difficulté de s'écarter du rapport d'expertise, le glissement de la responsabilité de l'autorité pénale vers l'expert est fréquente, d'une part quant à l'explication factuelle de la présence d'une trace, et d'autre part quant à la gestion des doutes. Au sein des tribunaux, il existe une tendance à transférer la question des doutes sur les scientifiques ou techniciens[531].

508 L'autorité pénale estime souvent qu'elle manque de compétence pour déterminer quelle valeur porter à l'incertitude. Par exemple, le résultat d'une analyse comparative d'ADN est de 98%, il faut déterminer quelle place laisser aux 2% non similaires. Les juristes ont tendance à se reposer sur l'expert pour qu'il détermine si la part d'incertitude de 2% doit être prise en considération dans la détermination de la valeur probatoire ou si elle est insignifiante.

509 Cette manière de procéder va à l'encontre de la répartition des rôles entre l'autorité pénale et l'expert. Ce dernier doit évaluer la valeur de l'incertitude en la quantifiant, mais il ne doit pas se déterminer sur l'impact de ce doute dans le cas d'espèce à juger. L'autorité pénale est la seule compétente pour accepter ou non le résultat d'expertise et lui donner la force probante qui lui revient.

510 La conséquence du transfert de la gestion des doutes à l'expert n'est pas anodine. L'autorité pénale qui devrait pouvoir s'écarter du rapport d'expertise et juger du poids à donner aux résultats s'en remet de plus en plus à l'avis de l'expert. Ce dernier n'étant présent aux procès que pour ses qualifications scientifiques ou techniques, il devrait renoncer à répondre à l'évaluation de l'incertitude. Néanmoins, il n'est pas juriste. C'est donc au juge que revient la tâche de ne pas s'écarter de ses devoirs et de conserver son plein pouvoir d'appréciation de la preuve pénale.

---

[529] StPO-DONATSCH, art.182 N 11.

[530] Infra Partie III, Chapitre 2, III, A, n° 2371 ss.

[531] VUILLE, RSC 2012, p. 7.

CHAPITRE 2: LES PREUVES FONDÉES SUR LES SCIENCES

511 Alors qu'auparavant l'ADN n'était pas considéré comme un indice, il est depuis 1984 fréquemment usité pour déterminer l'identité de l'auteur d'une infraction[532]. Plus récemment, la poussière a été analysée pour tenter de délimiter le lieu d'habitation du suspect, alors qu'il y a quelques années, elle n'était qu'une particule insignifiante pour l'enquête. Ces deux exemples illustrent que divers éléments semblant *a priori* insignifiants deviennent, grâce aux développements des sciences et plus particulièrement de la science forensique, des indices assortis d'une valeur probante.

512 Les empreintes au sens large pouvant provenir du corps – empreintes manuelles, palmaires, dentaires, auriculaires, épidermiques, génétiques, etc. –, d'une chose mobilière – empreintes pneumatiques, traces de peinture, débris automobiles, douilles, études balistiques, analyses des plaies, etc. –, d'une fibre – empreintes de vêtements ou de tout élément constitué de tissu ou de fibre –, ou de la découverte d'un ou de plusieurs poil(s), et les objets laissés par l'auteur de l'acte délictuel, les parasites, les poussières, les produits utilisés pour commettre une infraction – par exemple, le produit inflammable employé pour bouter le feu – ou toute autre trace n'entrant pas dans la catégorie des empreintes forment la famille des preuves indiciales[533]. Toutes ces marques laissées sur les lieux de l'infraction, sur le corps de la victime, dans le véhicule ou sur un objet ayant été en contact avec un individu sont des éléments essentiels à l'enquête et à la justice.

513 L'intérêt de la justice et de l'opinion publique a révélé l'importance des indices dans la procédure pénale moderne. Deux empreintes issues des preuves indiciales ont retenu particulièrement notre attention. L'une découle d'une technique centenaire et bien établie: l'empreinte papillaire, alors que l'autre, plus récente, fait encore débat: l'empreinte génétique. Notre chapitre consacré aux preuves fondées sur les sciences comporte donc deux parties traitant tour à tour de ces preuves, soit la dactyloscopie (I.) et l'acide désoxyribonucléique (II.).

[532] A ce sujet: LOCARD, T. I-II, p. 855. Supra Partie I, Chapitre 1, II, B, 2, b, n° 87 ss.

[533] LOCARD, T. I-II, p. 9; Message, CPP, p. 1194; SCHMID, Strafprozessrecht, p. 237.

I. La dactyloscopie

A. L'introduction

514 L'auteur ou les auteurs d'une infraction qui, notamment, manipulent un objet à mains nues, marchent à pieds nus ou appuient une partie découverte de leur corps sur un objet ou un élément intégré à la scène de crime laissent immanquablement leurs empreintes papillaires formés d'entrelacs et de crêtes.

515 L'étude des empreintes papillaires – du relevé à l'identification du propriétaire de l'empreinte – est nommée la *lophoscopie*[534]. Une section privilégiée de la *lophoscopie*, appelée la *dactyloscopie* – *dactylo-* provient du nom grec *dactulos* signifiant "doigt" et *-scopie* du nom *skopein* traduisible par le verbe "examiner" – s'intéresse uniquement aux crêtes épidermiques sises sur la pulpe des doigts.

516 En pratique, l'identification à l'aide d'une empreinte digitale est la plus usitée. C'est pourquoi, tout en n'ignorant point la preuve lophoscopique dans son ensemble dont les principes développés s'appliquent *mutatis mutandis*, la preuve dactyloscopique est au centre de notre écrit comme moyen probatoire permettant d'identifier le propriétaire de l'empreinte laissée sur une scène de crime.

1. Définition de l'empreinte papillaire

517 La structure de la peau humaine est complexe[535]. L'épiderme, couche superficielle de la peau, se renouvelle à l'aide du *stratum mucosum* – couche supérieure du derme – ou couche malpighienne (de Malpighi) qui contient des terminaisons nerveuses, des vaisseaux sanguins et des glandes nécessaires à la formation des dermatoglyphes visibles à la surface de la peau, et constitue la masse primaire des sillons cutanés. Formées de plis, plus ou moins parallèles et plus ou moins courbés, les crêtes épidermiques ou sillons cutanés dessinent l'empreinte papillaire. Grâce aux contaminations et aux sécrétions corporelles provenant des glandes

[534] MARGOT, LENNARD, Empreintes, p. 1-2.

[535] A ce sujet: CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 1 et 10-11; HOLDER, ROBINSON, LAUB-MACEO, Chapter 2-3 à 2-13; MARGOT, LENNARD, Empreintes, p. 2.

sudoripares eccrines et apocrines – la sueur –, ainsi que des glandes sébacées – le sébum – [536], le dessin des dermatoglyphes se dépose sur n'importe quelle surface et forme l'empreinte papillaire à relever.

518 La paume des mains, la plante des pieds, le front, les aisselles, les paupières, les mamelons, les parties génitales, la racine des poils et des cheveux sont les zones de la peau recouvertes du plus grand nombre de glandes sudoripares eccrines ou apocrines, ou de glandes sébacées. Cela étant, seules les surfaces internes des mains et des pieds bénéficient de crêtes papillaires. Tout contact de ces surfaces avec du verre, du papier, de la peau ou diverses autres surfaces transpose le dessin dermatoglyphe, ce qui permet d'obtenir fréquemment une trace analysable.

519 Dans le contexte juridique, outre la fréquence des dépôts analysables, l'empreinte papillaire revêt un intérêt particulier du fait qu'il a été théoriquement démontré qu'elle était immuable, inaltérable et individuelle tout en fournissant un résultat identificatoire scientifiquement probant après comparaison. Nous verrons, dans le cadre de la discussion sur ce moyen probatoire, que l'immuabilité, l'inaltérabilité et l'individualité sont des principes théoriques qui ne permettent en aucun cas d'assurer une identification, mais uniquement de créer une présomption d'identification[537]. Cela étant, dans cette partie introductive, nous nous limiterons à exposer les principes théoriques qui prévalent pour cette science.

a. L'immuabilité

520 La première qualité fondamentale des empreintes dermatoglyphes est leur immuabilité. Il ressort des travaux de William James Herschel qui a comparé ses empreintes et celles d'enfants ou d'autres adultes à plusieurs années d'intervalle, que les dessins dermatoglyphes ne changent pas avec les années[538]. Francis Galton complète cette étude en précisant que sur 296 points de référence sis sur les empreintes de huit sujets, aucun n'a disparu ou ne s'est modifié avec les années et aucune nouvelle crête ou bifurcation n'est apparue[539].

521 Alors que les dimensions de notre corps se modifient, notre peau se ride, nos cheveux blanchissent, du stade fœtal jusqu'à la mort et même au-delà, jusqu'à la putréfaction du

[536] A ce sujet: BUQUET, p. 33; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 106-107; HOLDER, ROBINSON, LAUB-MACEO, Chapter 2-11 à 2-13; KNOWLES, p. 714; MARGOT, LENNARD, Empreintes, p. 18.

[537] Infra Partie II, Chapitre 2, I, C, n° 636 ss.

[538] HERSCHEL, p. 76. Supra Partie I, Chapitre 1, II, B, 1, b, n° 74.

[539] CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 12.

cadavre ou sa crémation nos empreintes sont constantes et identiques dans leurs moindres détails[540]. Ce constat permet de comparer dans la durée des traces papillaires découvertes et une empreinte connue sans qu'il ne soit possible d'opposer une modification ou un changement des dessins dermatoglyphes.

b. L'inaltérabilité

522 Les dessins digitaux n'étant pas constitués à la surface de l'épiderme, contrairement à une croyance répandue, l'eau bouillante, le papier-émeri ou l'acide ne suffisent pas à faire disparaître les crêtes papillaires. Pour preuve, John Dillinger a essayé d'effacer ses dermatoglyphes en trempant ses doigts dans l'acide[541]. A sa mort, le FBI a prélevé ses empreintes digitales. Après comparaison avec le fichier des empreintes et malgré le traitement à l'acide subi, il a été constaté que les crêtes papillaires étaient restées intactes et inchangées. Ce n'est qu'en altérant les papilles dermiques par un sévère endommagement des téguments qu'un changement de la structure des arêtes dessinant les empreintes intervient. Robert Phillips a employé la chirurgie plastique pour remplacer la peau des pulpes digitales par des greffons prélevés sur son torse[542]. Après cicatrisation, la peau a grandi avec de nouvelles empreintes digitales. Cependant, lors de l'analyse des traces découvertes sur la scène de crime, les dessins dactyloscopiques de la pulpe des doigts ne sont pas les seuls analysés; grâce aux empreintes de ses secondes phalanges non-endommagées, il a été possible de confondre Robert Phillips.

523 Relevons encore que les blessures superficielles ne touchant que l'épiderme transforment que temporairement les caractéristiques digitales. Les entailles plus profondes peuvent créer des cicatrices coupant le dessin originel, mais ne le modifiant pas pour autant puisque le tissu cicatriciel se situe au niveau de l'épiderme et non du derme[543].

524 Les empreintes digitales sont donc inaltérables nonobstant l'hypothèse invraisemblable d'une greffe complète de la peau du corps humain. Quant aux cicatrices qui ne changent en rien le dessin dermatoglyphe, elles n'empêchent pas l'identification dactyloscopique. Au contraire, elles ont l'avantage d'offrir une caractéristique supplémentaire visible à l'œil nu et utile pour identifier le propriétaire d'une trace papillaire.

---

[540] CHAMPOD, Reconnaissance, p. 6; DESBROSSE, p. 52; LOCARD, T. I-II, p. 86; WERTHEIM, p. 96.

[541] GASCOYNE-BOWMAN, p. 9; MATERA Dary, *John Dillinger: The Life And Death Of America's First Celebrity Criminal*, New York 2004; TILSTONE, SAVAGE, CLARK, p. 153.

[542] HAMILTON Sue, *Fingerprint analysis – Hints from prints*, Edina 2008, p. 6.

[543] A ce sujet: CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 12; MARGOT, LENNARD, Empreintes, p. 3.

c. L'individualité

525 L'individualité des empreintes digitales apporte la dernière pierre nécessaire pour affirmer que ce moyen de preuve a une valeur identificatoire notable.

526 L'unicité des empreintes papillaires est la conséquence de la morphogénèse se déroulant durant la vie fœtale[544]. Dès la onzième jusqu'à la vingt-quatrième semaine, des bosses formées d'un pore se développent sur les parties tactiles et grandissent à vitesse variable. Les papilles sont le résultat du fusionnement de ces pores qui forment alors une ligne en arc, en boucle, en verticille ou composite pouvant, selon les formes, se composer d'aucun, d'un ou de plusieurs delta[545].

527 L'hérédité est également un facteur d'influence quant à la formation du dessin papillaire sans pour autant permettre l'identification à l'aide des ascendants ou descendants[546]. En outre, les minuties – appelées également points caractéristiques, points de Galton ou points d'identité – conditionnées par le stress et autres pressions variables, et d'éventuelles cicatrices complètent la formation individuelle des empreintes papillaires.

528 La conséquence de ce processus aléatoire est l'infinité des formes, du nombre et des dispositions des crêtes papillaires[547]. Les calculs de Francis Galton affirment qu'il existe une chance sur 64 milliards de découvrir la même empreinte sur deux individus différents. Ce chiffre doit néanmoins être relativisé, puisque cette probabilité est influencée par le nombre de points de comparaison; plus ce nombre est grand, moins il existe de chance de découvrir une même empreinte appartenant à deux individus différents. Au surplus, dans sa thèse, Galdino Ramos calcule qu'en comparant une vingtaine de points et en tenant compte du nombre de terriens, il faudrait près de 5 millions d'années pour découvrir deux dessins identiques[548]. Pratiquement, comme en théorie selon les calculs, il est donc impossible de retrouver la même configuration des minuties chez deux individus offrant ainsi un pouvoir

---

[544] BECUE, CHAMPOD, EGLI, MARGOT, p. 10; CHAMPOD, Friction Ridge Skin, p. 112; HOLDER, ROBINSON, LAUB-WERTHEIM, Chapter 3-4 à 3-18; MARGOT, CHAMPOD, p. 231; WERTHEIM, p. 96.

[545] A ce sujet: BUQUET, p. 82 ss; CHAMPOD, Reconnaissance, p. 8 ss; CHAMPOD, Friction Ridge Skin, p. 111-112; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 17 ss; HENRY, p. 14 ss; JERLOV, p. 270 ss; KNOWLES, p. 713; LOCARD, T I-II, p. 44 ss, p. 395 ss et p. 431 ss; MARGOT, LENNARD, Empreintes, p. 4 ss; PISANI, p. 20.

[546] BECUE, CHAMPOD, EGLI, MARGOT, p. 10; CHAMPOD, Reconnaissance, p. 11; HOLDER, ROBINSON, LAUB-WERTHEIM, Chapter 3-18 à 3-20; LOCARD, T. I-II, p. 89-93.

[547] CHAMPOD, Friction Ridge Skin, p. 112; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 13; MARGOT, CHAMPOD, p. 230.

[548] A ce sujet: LOCARD, T. I-II, p. 88.

identificatoire à une trace papillaire. Les descripteurs additionnels, comme la "ligne comptée" ou *"ridge counting"* et la "ligne tracée" ou *"ridge tracing"* complètent l'analyse décadactylaire traditionnelle pour augmenter le pouvoir descriptif et permettre une individualisation encore plus probante.

529 A noter qu'en fonction de la forme générale des stries et des particularités des minuties, le dessin papillaire est plus ou moins intéressant pour permettre une comparaison adéquate et probante[549]. Par exemple, la forme en arc d'une empreinte dactyloscopique ou palmaire n'ayant pas de delta n'a pas de particularité signifiante, hormis l'îlot; alors que les formes en bideltes sont plus variées et offrent des points caractéristiques en abondance.

2. Le prélèvement et l'analyse des empreintes papillaires

530 Aucune identification papillaire ne peut être faite sans comparaison entre une fiche et une trace découverte. Le travail de la police criminelle et scientifique en dactyloscopie est de rechercher et de révéler les traces papillaires (a.), de les analyser (b.) et, si la trace revêt une qualité suffisante, d'activer le processus d'identification (c.).

a. La recherche et la révélation des empreintes

531 L'expérience démontre que l'empreinte découverte sur la scène de crime ou sur un objet relatif au cas criminel peut se présenter sous trois aspects différents[550]:

- les empreintes visibles obtenues lorsqu'une personne laisse, par exemple, sa main apposée sans bouger et/ou sans écraser la surface, ce qui est rarement le cas. Généralement, ce type d'empreinte ressemble plus à une tâche qu'à une trace, mais conserve un intérêt pour fournir la dimension et la forme de la main, du pied ou du doigt;
- les empreintes moulées, qui ont l'avantage de fournir une image en trois dimensions du dessin papillaire;
- et les empreintes latentes, qui doivent être traitées et révélées pour être utilisables.

[549] CHAMPOD, Friction Ridge Skin, p. 112; EXPERT WORKING GROUP, p. 2.

[550] A ce sujet: CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 105; EXPERT WORKING GROUP, p. 1; LOCARD, T. I-II, p. 119-121; MARGOT, LENNARD, Empreintes, p. 15-16.

532 Toutes les recherches d'empreintes se focalisent sur la localisation et la détection de ces trois types de traces indiciales.

533 L'expert scientifique désirant relever une empreinte doit respecter une marche à suivre afin de garantir le traitement optimal d'une trace indiciale. Avant tout prélèvement et analyse, il doit se poser trois questions: "La pièce ou la surface sur laquelle est déposée une empreinte est-elle transportable?", "L'empreinte est-elle visible?" et "L'objet a-t-il été contaminé par une cause environnementale?". Si l'objet est petit ou si la pièce est transportable, l'expert déplace l'indice de la scène du crime en prenant les précautions nécessaires pour permettre un traitement idéal au laboratoire. En revanche, si l'objet n'est pas transportable, il analyse l'empreinte sur les lieux. Ensuite, il répond à la deuxième interrogation. Si la réponse est positive, il photographie la trace, puis procède à son examen; au contraire, si la réponse est négative, il se doit de choisir la meilleure méthode, en déterminant le choix des techniques à sa disposition et les possibilités d'utiliser des techniques en séquence pour traiter et révéler l'empreinte[551]. Dans l'hypothèse où la réponse à la troisième question est positive, la détection doit se limiter aux dépôts papillaires non affectés; si la réponse est négative, il procède au relevé complet.

534 Ainsi, le processus de prélèvement peut varier selon le type de glande qui a sécrété les résidus, le type d'empreinte et la surface sur laquelle elle est déposée. Le choix de la méthode influe directement sur la valeur du résultat identificatoire, une détection adéquate fournit un résultat plus probant[552].

535 L'empreinte visible étant facilement détectable, il est suffisant d'utiliser une source luminescente variée – lampe UV, laser, lumière filtrée ou lumière blanche intense – pour renforcer la clarté et la photographier[553].

536 L'empreinte moulée est généralement révélée par une source lumineuse optimale, corrélativement à ce qui prévaut pour l'empreinte visible, ou par moulage. Cette seconde technique s'illustre par l'usage d'un moulage dentaire en silicone qui révèle l'image en 3D permettant de faciliter la photographie de l'empreinte[554].

---

[551] BECUE, CHAMPOD, MARGOT, p. 10-18; BECUE, CHAMPOD, EGLI, MORET, p. 16-36; KNOWLES, p. 715; MARGOT, LENNARD, Empreintes, p. 20-21.

[552] CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 105; DONOVAN, p. 204; MARGOT, LENNARD, Empreintes, p. 16.

[553] A ce sujet: CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 171; HOLDER, ROBINSON, LAUB-YAMASHITA, FRENCH, Chapter 7-2 à 7-50.

[554] CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 171; HOLDER, ROBINSON, LAUB-YAMASHITA, FRENCH, Chapter 7-2 à 7-50; MARGOT, LENNARD, Empreintes, p. 16.

537 La révélation de l'empreinte latente est plus problématique dès lors qu'elle est invisible ou presque à l'œil nu et qu'une erreur de sélection dans la méthode peut ruiner toute possibilité de détection, subséquemment d'analyse. Il existe quatre types de méthodes de détection pouvant se combiner: les méthodes optiques qui préservent adéquatement les sécrétions déposées; les méthodes physiques qui ne sont viables que pour des empreintes récentes et nécessitent l'usage d'un pinceau qui peut détériorer la trace par brossage; les méthodes chimiques qui permettent de révéler les empreintes sur des supports poreux longtemps inexploitables et d'augmenter le contraste obtenu suite à une technique physique; et les méthodes physico-chimiques qui relèvent le contraste afin d'obtenir un dessin papillaire plus clair et permettre une meilleure comparaison[555].

538 Dépendamment de la surface, de l'âge de l'empreinte, voire de l'humidité, l'expert choisit le moyen le plus adéquat pour renforcer le contraste des empreintes digitales, palmaires et plantaires sans les endommager. Il ne peut pas privilégier une technique plutôt qu'une autre avant d'avoir analysé les lieux du crime. En outre, des connaissances en physique, particulièrement en photoluminescence, en ondes et en absorption ou réflexion de la lumière, ainsi qu'en chimie sont nécessaires pour appréhender correctement les techniques de détection d'empreintes. Pour un juriste, la compréhension des principes chimiques ou physiques n'est pas nécessaire, c'est pourquoi nous ne nous attardons pas sur ce sujet. Néanmoins, dès lors que les qualifications de l'expert, les méthodes employées et le degré de clarté de l'empreinte dévoilée – contraste, révélation des crêtes, préservation, etc. – jouent un rôle pour déterminer la valeur probatoire d'une trace papillaire, extensivement sa valeur identificatoire, tout juriste doit s'intéresser un minimum à l'aspect technique se cachant derrière un résultat identificatoire.

b. L'analyse

539 La première phase du processus de l'identification par les crêtes dermatoglyphes est l'analyse, examen minutieux de l'inconnu – les empreintes n'étant ni identifiées, ni identifiables[556]. Cette étape sert à déterminer objectivement les informations apportées par les lignes papillaires révélées en prenant en considération les crêtes papillaires, la clarté de l'image, la possible altération de la trace, les techniques de détection et la pression.

---

[555] A ce sujet: BUQUET, p. 39; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 111, 114 et 172-173; HOLDER, ROBINSON, LAUB-YAMASHITA, FRENCH, Chapter 7-2 à 7-50; MARGOT, LENNARD, Empreintes, p. 50, 60 et 111-113; MARGOT, LENNARD, RIPC, p. 11.

[556] CHAMPOD, Fingerprint, p. 1-4; WERTHEIM, p. 99.

540 L'analyse par l'expert se réalise en trois étapes correspondant aux trois niveaux d'informations fournies par une empreinte[557]: la tendance générale du dessin ne requérant pas d'agrandissement; l'agrandissement de cinq à dix fois permettant à l'expert de se concentrer sur les dimensions physiques des crêtes et sur les minuties, et de noter les marques laissées par d'éventuelles verrues, cicatrices, plis ou rides, et l'agrandissement maximal pour dévoiler des détails infimes ne concernant généralement qu'une seule crête[558].

541 Durant l'analyse, l'expert doit tenir compte des différences pouvant intervenir entre une image en deux ou en trois dimensions, des distorsions pouvant résulter de diverses sources telles que le sens ou la pression du toucher, la surface du dépôt, voire la durée de contact, ainsi que du degré de clarté de l'impression puisque les altérations peuvent diminuer fortement le pouvoir et la certitude identificatoire[559]. Toutes les étapes de l'analyse et tous les points forts et/ou faibles de l'image prélevée doivent apparaître dans le rapport d'expertise afin de permettre aux magistrats d'apprécier correctement l'indice dactyloscopique[560]. Sans ces indications, le rapport d'expertise est incomplet ou tout du moins ne permet ni à la défense, ni à l'accusation, ni même au magistrat de se faire une idée exacte de la démonstration apportée par la preuve dactyloscopique.

c. Le processus identificatoire de la comparaison à l'achèvement

542 En tenant compte des détails délivrés par l'analyse, l'expert recherche par tâtonnement une empreinte compatible – connue et identifiée – avec la trace découverte sur la scène de crime ou sur un objet relié à celle-ci. Il doit évaluer objectivement la correspondance entre les deux images et se déterminer sur leur ressemblance sans avoir une vue préconçue ou un espoir.

i. L'assistance des outils automatisés

543 Au commencement des fiches signalétiques, la comparaison s'effectuait manuellement. Les systèmes de classement créés à l'époque et basés sur les similarités générales des empreintes ont permis de diminuer considérablement le nombre de comparaisons à effectuer et la durée

[557] CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 16.

[558] CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 16; WERTHEIM, p. 99.

[559] CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 18-20; WERTHEIM, p. 99.

[560] ASHBAUGH, p. 79; WERTHEIM, p. 100.

d'analyse. Le *continuum*[561] des dessins papillaires généraux issu des travaux de Jan Evangelista Purkinje (1823), Francis Galton (1892), Edward Henry (1900) ou Juan Vucetich (1904) pour les empreintes dactyloscopiques, de Eugène Stockis, Antonio Lecha-Marzo et Vincente Rodriguez Ferrer pour les empreintes palmaires, et ceux d'Harris Hawthorne Wilder et Bert Wentworth pour les empreintes plantaires est aujourd'hui approuvé par les informaticiens qui ont développé des bases de données afin de classifier automatiquement les empreintes papillaires et de pouvoir aisément les comparer. L'empreinte digitale dite d'entrée – se rapportant à la trace à identifier – est assortie à un sous-ensemble de dessins papillaires de la base de données, ce qui permet de réduire le temps et la complexité de la recherche automatisée.

544 En Suisse, le fichier AFIS effectue simultanément, en quelques minutes, une recherche sur les traces relevées sur les lieux de l'acte délictuel – provenant d'un ou de plusieurs doigts, voire des dix doigts, des empreintes de la paume et de la tranche de la main – et permet ensuite d'identifier une personne de manière fiable[562]. Grâce à ce moyen informatique, il est possible également de comparer une empreinte avec une autre, une trace avec une empreinte ou deux traces entre elles.

545 Le processus d'identification préconise en premier lieu de débuter l'analyse par une vérification visuelle de la viabilité du dessin papillaire. Lors du *quality-check*, l'expert scientifique contrôle la clarté de l'image et l'existence de points caractéristiques. L'examinateur compare manuellement l'empreinte inconnue avec les dessins papillaires de la victime, des témoins et des potentiels suspects. En cas de comparaisons infructueuses, les moyens informatiques sont usités. L'empreinte inconnue est alors scannée puis entrée dans la base de données AFIS afin d'effectuer une recherche automatisée pour réduire le nombre de donneurs possibles.

546 Le système informatique compare l'empreinte numérisée avec toutes les données enregistrées en ciblant sa recherche sur les caractéristiques générales relevant de l'analyse de premier niveau, sélectionne certaines fiches en codifiant et en interprétant – grâce aux algorithmes et à l'extraction des minuties – les traces papillaires et propose une liste de candidats pertinents[563]. L'AFIS est donc inefficace pour individualiser avec une certaine certitude une

---

[561] BUQUET, p. 82-83; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 17; KNOWLES, p. 713; LOCARD, T. I-II, p. 44-46, p. 395 et p. 407; MARGOT, LENNARD, Empreintes, p. 4.

[562] Informations disponibles sur le site internet de l'Office fédéral de la police : http://www.fedpol.admin.ch [consulté le 08.05.2016].

[563] BUQUET, p. 42; DESBROSSE, p. 57.

empreinte. Son rôle se limite à diminuer la charge de travail des scientifiques en restreignant le nombre d'empreintes à confronter.

547 Le potentiel d'AFIS ne se borne pas à comparer des empreintes, la confrontation entre une trace et l'empreinte papillaire du suspect, d'une empreinte connue – notamment celle du suspect – avec les traces inconnues du fichier, d'une trace détectée avec les traces inconnues pour lier deux ou plusieurs infractions entre elles, ou pour identifier une personne inconnue sont des exploitations possibles du système automatisé[564].

548 Relevons encore que le fichier AFIS offre la possibilité d'utiliser le signalement décadactylaire ou l'identification monodactylaire pour les empreintes digitales. Le premier identifie un être humain sur la base de l'empreinte de ses dix doigts. Plus fréquemment, le dessin papillaire d'un seul doigt, tout en ignorant lequel, est découvert sur une scène de crime. Dans de telles circonstances, la comparaison est effectuée à l'aide du fichier monodactylaire regroupant une sélection d'empreintes séparées des individus fichés et des traces stockées. Cette comparaison permet de confondre deux empreintes sans nécessairement avoir la trace des dix doigts ayant pour effet une meilleure rationalisation du fichier AFIS et de l'usage des empreintes digitales.

ii. La comparaison manuelle

549 Lorsque le fichier AFIS ne fournit aucune concordance même à hauteur d'une dissemblance, la trace est exclue. Au contraire, si la comparaison est possible, l'expert poursuit en confrontant les empreintes listées par AFIS avec l'empreinte de comparaison à l'aide des caractéristiques papillaires de deuxième niveau.

550 L'examinateur recherche des points visibles de la trace – en regardant le sens, la position, ainsi que la longueur des lignes papillaires, les cicatrices ou les plis de flexion –, sélectionne deux ou trois points caractéristiques et les confrontent avec les points visibles de l'empreinte de référence[565]. Il réitère cette manœuvre jusqu'à ce que toutes les minuties visibles et nécessaires à l'identification aient été analysées et comparées.

551 Suite à l'analyse de deuxième niveau et lorsque les minuties concordent en vertu de leur forme et de leur position, l'expert poursuit en examinant les caractères de troisième niveau d'analyse, tels que les pores ou crêtes papillaires. Ce processus d'analyse de concert avec

[564] LEMAN-LANGLOIS, BRODEUR, p. 75; MARGOT, LENNARD, Empreintes, p. 12-13.

[565] ASHBAUGH, p. 89; BUQUET, p. 34; CHAMPOD, Reconnaissance, p. 12.

celui de second niveau a l'avantage de posséder un pouvoir identificatoire accru. Plus les détails sont nombreux, plus l'individualisation de l'empreinte est précise et certaine.

552 Une fois l'analyse de deuxième et troisième niveau effectuée par un premier expert, un second examinateur réalise le même processus. La validation des résultats obtenus par la recherche automatisée et l'établissement de la corrélation entre les points concordants sont donc effectués manuellement par deux examinateurs scientifiques successifs.

iii. Le résultat identificatoire

553 Une même empreinte ne peut fournir deux images identiques[566], puisque tout contact entre la pulpe du doigt, la paume de la main ou la voûte plantaire avec une surface plane laisse une trace qui varie selon la pression, l'angle, la zone de contact, ainsi que selon la nature de la surface. Le résultat identificatoire est donc une simple évaluation de la concordance. En d'autres termes, il est la conclusion de l'analyse réalisée par l'examinateur qui considère les similitudes et les différences et se réfère à tous les éléments qui apparaissent dans chaque image dermatoglyphe pour fonder son résultat.

554 Dans les faits, une empreinte claire, nécessitant une analyse minimum ou contenant des détails uniques suffisants est évaluée au cours de la phase de comparaison. Dans les autres cas – manque de clarté, de détails caractéristiques ou comprenant des altérations –, la zone d'ombre oblige un minimum d'attention pour identifier le propriétaire des dermatoglyphes en éliminant les profils concordants, mais non similaires. Pour se faire, l'expert détermine s'il existe des concordances entre l'empreinte inconnue et celle connue et s'il peut conclure à une unicité.

555 Une dissemblance entre deux dessins papillaires n'est pas synonyme d'exclusion, exception faite des dissemblances liées aux caractéristiques de premier niveau. En revanche, l'empreinte est écartée si aucune similitude n'existe. A noter que, l'empreinte papillaire pouvant servir de preuve identificatoire, le niveau de connaissances, l'expérience et la technique d'identification employée doivent être suffisants pour effectuer une analyse quantitative et qualitative correcte du dessin dermatoglyphe[567] et permettre de déterminer l'influence des altérations ou des dissemblances. Un expert confirmé peut notamment analyser des empreintes complexes qui ne sont pas à la portée de l'examinateur novice.

[566] CHAMPOD, Reconnaissance, p. 12; WERTHEIM, p. 101.

[567] ASHBAUGH, p. 93 et 94; CHAMPOD, Reconnaissance, p. 16; CHAMPOD, Friction Ridge Skin, p. 113; MARGOT, CHAMPOD, p. 64.

L'expérience et la technicité de l'identification ne sont donc pas à négliger pour décréter la force probante du résultat identificatoire.

556 Le second expert effectuant la même analyse doit parvenir à un résultat identique ou du moins fortement similaire. L'avis identificatoire revenant aux seuls experts, il est nécessaire que tous deux arrivent à un résultat positif pour décréter qu'il y a identification; dans l'hypothèse où l'un, l'autre ou les deux concluent à l'impossibilité d'identifier le propriétaire de l'empreinte, il n'y a pas d'identification. Dans le cas où un doute subsiste, il doit profiter au donneur de l'empreinte ou, tout du moins, il est nécessaire d'effectuer d'autres recherches si les détails ou leur qualité ne permettent pas de fournir un avis identificatoire.

557 Concernant le résultat identificatoire, il n'est probant que si un certain nombre de similarités existent entre les deux empreintes comparées. Edmond Locard a déterminé que s'il existe plus de douze points concordants, l'empreinte est déclarée nette et la certitude d'identité est reconnue. Si huit à douze minuties similaires sont répertoriées, la certitude dépend de la netteté de l'empreinte, de la rareté de ce type de points caractéristiques, de la présence d'un delta ou d'un centre, de la présence d'un pore, de la largeur, de la direction ou de l'angle des bifurcations et des crêtes papillaires[568]. Lorsque le nombre de concordances est en deçà de huit, aucune certitude n'est donnée, il n'existe qu'une présomption. En outre, l'observation de la netteté des points et l'analyse de leur fréquence permet d'augmenter la probabilité d'une concordance[569], extensivement des possibilités identificatoire même si moins de huit minuties similaires sont analysables.

558 Cela étant, nous en parlerons dans le cadre de notre discussion sur la valeur probatoire des empreintes digitales, les experts forensiques préconisent non pas l'emploi d'un standard minimum, mais un examen et/ou une analyse concrète de la quantité des minuties concordantes et de leur qualité afin de fournir un pourcentage d'identification ainsi que de couplé ces principes scientifiques avec un professionnalisme et une expérience adéquats[570].

---

[568] LOCARD, T. I-II, p. 222.

[569] CHAMPOD, Reconnaissance, p. 13.

[570] CHAMPOD, Fingerprint, p. 4-7; CHAMPOD, Friction Ridge Skin, p. 113 et 115-116; CHAMPOD, Overview, p. 306-308; NATIONAL RESEARCH COUNCIL, p. 208 et 217 ss.

B. Les notions juridiques

559 Lorsque les autorités soupçonnent qu'une infraction a été commise (art. 197 et 260 al. 1 CPP), elles peuvent prélever des traces ou des données signalétiques dans le but d'établir les faits de l'acte délictuel et d'identifier l'auteur[571].

560 Pour encadrer le travail de l'autorité judiciaire et de la police ainsi que pour respecter les prérogatives liées à l'administration des preuves et à la restriction des droits fondamentaux, la Suisse a légiféré sur les mesures d'investigation, notamment sur la prise d'empreintes papillaires, l'analyse des données, la transmission et la conservation des informations.

1. Le cadre légal

a. L'atteinte aux droits fondamentaux du prélèvement et de l'analyse des données signalétiques

561 La liberté personnelle est une liberté centrale qui protège la personne humaine tant en ce qui concerne sa liberté de mouvement que dans toutes les manifestations élémentaires de la personnalité humaine, soit dans son intégrité psychique et physique[572]. Le droit à l'intégrité physique protège spécifiquement les individus contre les interventions étatiques sur le corps des personnes[573].

562 Dans sa jurisprudence constante[574], le Tribunal fédéral reconnaît que le relevé des données personnelles par la police, notamment des empreintes digitales, constitue une atteinte à la liberté personnelle, plus particulièrement à la sphère intime de l'individu, et au droit de la personnalité protégé par la Constitution. Le prélèvement des données signalétiques n'étant pas invasif, cette mesure ne constitue toutefois qu'une atteinte légère[575]. En revanche, l'utilisation et le stockage des données signalétiques peut, notamment par la durée de la

---

[571] Message, CPP, p. 1225; TARONI, Thèse, p. 13.

[572] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 143-144; GRABENWARTER, PABEL, p. 230; GRISEL A., p. 550 ss; HARRIS, O'BOYLE, WARBRICK, p. 366-368; MÜLLER, SCHEFER, p. 57 ss.

[573] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 149; GRABENWARTER, PABEL, p. 230; HARRIS, O'BOYLE, WARBRICK, p. 361 et 366-367; RAINER, p. 692.

[574] ATF 107 Ia 138 = JdT 1982 IV 147; ATF 109 Ia 146, 155; ATF 113 Ia 257, 263; ATF 120 Ia 147, 149 = JdT 1996 IV 61; ATF 128 II 259, 268; ATF 136 I 101 = JdT 2010 I 367; ATF 138 I 256, 258 = JdT 2012 I 102.

[575] ATF 107 Ia 138, 145 = JdT 1982 IV 147, 151; ATF 128 II 259, 270; ATF 134 III 241, 247 = JdT 2009 I 411; CPP-Commentario-BERNASCONI, art. 260 N 11; SCHMID, Praxiskommentar, art. 260 N 9.

conservation ou l'emploi des données[576], causer une atteinte de plus forte importance – allant de légère à grave – à la liberté personnelle et au droit à l'autodétermination informationnelle protégés par la Constitution fédérale (art. 8 § 2 CEDH, art. 17 § 1 Pacte II et art. 10 et 13 Cst).

563 Partant du constat qu'il existe une atteinte en cas de prélèvement, d'analyse et d'enregistrement des données personnelles, la personne concernée par la prise d'empreintes papillaires peut se prévaloir des droits constitutionnels et des droits de la personnalité[577].

564 Par conséquent, lorsque l'autorité pénale est désireuse d'employer l'identification grâce aux empreintes papillaires, la mesure doit reposer sur une base légale, être justifiée et proportionnée. Relevons ici que l'atteinte étant de peu de gravité, le prélèvement et le processus d'identification des empreintes digitales, palmaires et plantaires peut se fonder sur une loi formelle ou une loi au sens matériel[578].

b. Les dispositions suisses sur les données signalétiques

565 En tant que mesure de contrainte, soit un acte procédural portant atteinte aux droits fondamentaux (art. 196 CPP), le prélèvement et le traitement subséquent des empreintes doivent respecter les conditions de restriction des droits fondamentaux (art. 36 Cst) et celles – générales – de la prise d'une mesure de contrainte (art. 197 CPP).

566 Jusqu'en janvier 2011, la prise d'empreintes digitales, extensivement palmaires ou plantaires, était légitimée par les dispositions légales cantonales sur la police et/ou, dans de rares cantons, de procédure pénale. Avec l'entrée en vigueur du Code de procédure pénale unifié, le prélèvement et l'analyse des données signalétiques sont régis par ledit Code (art. 260-261 CPP). Comme auparavant avec les normes cantonales, l'Ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques (AFIS-O) complète la législation en matière de prélèvement et de saisie des données signalétiques[579].

---

[576] ATF 113 Ia 257, 263-264; ATF 128 II 259, 270 = JdT 2003 I 411.

[577] ATF 104 Ia 35, 39-40 = JdT 1979 IV 150, 154-155; ATF 107 Ia 138, 145 = JdT 1982 IV 147, 151; ATF 113 Ia 257, 263; ATF 120 Ia 147, 149 = JdT 1996 IV 61; ATF 128 II 259, 268; ATF 136 I 101 = JdT 2010 I 367; ATF 138 I 256, 258 = JdT 2012 I 102.

[578] AUER, HOTTELIER, MALINVERNI, Vol. II, p. 185; GRISEL E., p. 29-30; MÜLLER, SCHEFER, p. 170-171.

[579] Ordonnance fédérale du 21 novembre 2001 sur le traitement des données signalétiques biométriques (AFIS-O), RS 361.3.

567 Les dispositions légales édictées traitent toutes des données signalétiques. Par ces termes, le législateur entend "*toutes caractéristiques extérieures d'un être humain pouvant être mesurées ou constatées*"[580]. Les empreintes digitales, palmaires et plantaires pouvant être constatées ou prélevées par le biais de révélateurs optiques, chimiques, physiques ou physico-chimiques, ainsi que mesurées et caractérisées à l'aide des pores et minuties présents dans le dessin dermatoglyphe, il s'agit bien de données signalétiques et les articles concernant ces données trouvent à s'appliquer.

i. La saisie des empreintes papillaires

a) Le champ d'application matériel et personnel

568 Une trace papillaire retrouvée sur une scène de crime n'a de possible valeur identificatoire que si elle peut être comparée avec des empreintes papillaires, et, mieux, encore des empreintes dont l'identité du propriétaire est connue.

569 La saisie des données signalétiques est réglementée à l'art. 260 CPP. Par "*saisie*", il faut comprendre le processus strict du prélèvement de données, dès lors que l'utilisation et le stockage sont réglementés à l'art. 261 CPP.

570 Contrairement aux art. 255 al. 1, 269 al. 1 et 2, 281 al. 4 et 282 al. 1 let. a CPP, les art. 260 et 261 CPP sont muets sur les conditions matérielles de saisie des données signalétiques et s'agissant des personnes à propos desquelles un tel prélèvement peut intervenir. Il faut, par conséquent, se référer à la disposition générale de l'art. 197 CPP et à la volonté du législateur. S'agissant d'une mesure non-invasive, la saisie d'empreinte papillaire ou de toutes autres données signalétiques n'est pas limitée à l'existence de soupçons de perpétration d'un crime ou d'un délit, mais s'étend aux contraventions, le critère déterminant étant la gravité de l'infraction justifiant la saisie des données (art. 197 al 1 let. d CPP). Lorsque les autorités pénales soupçonnent qu'une infraction a été perpétrée et si la saisie des données signalétiques respecte la subsidiarité[581] et est justifiée au regard de la gravité de l'infraction, elles sont autorisées, notamment, à prélever les empreintes digitales d'un individu.

[580] BSK-StPO-WERLEN, art. 260-262 N 3-4; Message, CPP, p. 1225; Polizeiliche Ermittlung-ALBERTINI, SCOSSA-BAGGI, p. 397; StPO-HANSJAKOB, art. 260 N 1.

[581] ATF 109 Ia 146, 155.

571 Le Conseil fédéral indique que la saisie des données signalétiques peut être entreprise sur le prévenu et sur des individus qui ne sont ni soupçonnés, ni prévenus d'une infraction, notamment pour écarter les traces indiciales laissées par les occupants légitimes sur les lieux de l'infraction ou par de simples témoins[582].

572 Si ni l'art. 260, ni l'art. 261 CPP ne limitent le champ d'application personnel de la saisie des données signalétiques, et si le législateur ouvre l'exploitation de cette mesure de contrainte contre des personnes ni prévenues ni soupçonnées, il ne faut cependant pas perdre de vue l'art. 197 al. 1 let. b CPP. Cette disposition instaure qu'une mesure coercitive ne peut pas être appliquée sans soupçons suffisants et solides sur l'existence de faits délictuels et sur l'implication du suspect dans la commission de l'infraction[583], condition faisant défaut si la personne n'est pas suspectée ou prévenue. Pour pallier ce déficit, la prise d'empreintes n'est acceptable qu'en respectant rigoureusement le principe de proportionnalité (art. 197 al. 2 CPP) et ce en considérant la gravité de l'infraction, ainsi que la difficulté d'établir les faits par d'autres méthodes[584].

573 Ainsi, la présence de soupçons sur l'implication de la personne concernée par la prise d'empreintes digitales est préférable, mais non nécessaire. Néanmoins, dans le dessein d'exclure les opérations de *fishing*[585], les soupçons d'action doivent obligatoirement exister. Dans ce cadre, le prélèvement permettant de disculper, inculper ou cibler les traces inconnues remplit indirectement la condition de soupçons et permet l'établissement des faits.

b) La compétence pour ordonner la saisie

574 Autre conséquence de la qualification d'atteinte légère aux droits fondamentaux, la saisie des empreintes papillaires est de la compétence des tribunaux, du ministère public et également de la police (art. 260 al. 2 CPP et explicitement prévu à l'art. 206 al. 1 CPP pour la police). Généralement, l'ordre est donné sous la forme d'un mandat écrit brièvement motivé, mais, en

---

582 CPP-Commentario-BERNASCONI, art. 260 N 6-7; CR-CPP-ROHMER, art. 260 N 13-14; EICKER, HUBER, p. 175; JOSITSCH, Strafprozessrechts, p. 138-139; Message, CPP, p. 1225; MOREILLON, PAREIN-REYMOND, art. 260 N 10; RIKLIN, Strafprozessordnung, art. 260 N 5; SCHMID, Handbuch, p. 477.

583 ATF 116 Ia 143, 146 = JdT 1992 IV 120,121; ATF 134 II 318, 327; ATF 136 IV 82, 85; ATF 137 IV 122, 126; TF 1B_322/2013 du 20 décembre 2013, c. 3.1; TF 1B_487/2012 du 18 février 2013, c. 3.5; PIETH, p. 118 ; StPO-HUG, SCHEIDEGGER, art. 197 N 5-6.

584 MOREILLON, PAREIN-REYMOND, art. 250 N 10; Polizeiliche Ermittlung-ALBERTINI, SCOSSA-BAGGI, p. 401; Rapport explicatif relatif à l'avant-projet, p. 193; SCHMID, Handbuch, p. 477; SCHMID, Praxiskommentar, art. 260 N 6.

585 ATF 129 II 462, 467-468 = JdT 2005 IV 29, 33-34; ATF 134 II 318, 327; ATF 136 IV 82, 85; PIETH, p. 119.

cas d'urgence, la saisie est ordonnée oralement puis confirmée et motivée par écrit (art. 260 al. 3 CPP).

575 Le processus d'identification étant relativement long, l'attente liée à l'établissement d'un mandat écrit n'influe que peu sur la durée du traitement lophoscopique[586], ce qui restreint les cas d'urgence.

c) Le refus et les voies de recours

576 La personne concernée par le relevé anthropométrique doit toujours se soumettre à l'adjonction. En cas de refus relatif à la saisie de données signalétiques décidée par la police[587], le ministère public a le pouvoir d'ordonner le prélèvement (art. 260 al. 4 CPP), décision soumise au recours (art. 393 al. 1 let. a CPP) à l'instar de la saisie ordonnée directement par le procureur, étant précisé que la personne concernée ne doit pas obligatoirement être informée de la possibilité de refuser le prélèvement[588].

577 Lorsque la direction de la procédure ordonne la saisie, il semble que le recours ne soit pas ouvert (art. 393 al. 1 let. b *in fine* CPP)[589]. Le législateur a, par cette disposition, voulu éviter l'interruption des débats[590]. La problématique est qu'en cas d'urgence une mesure de contrainte peut être ordonnée par la direction de la procédure en première instance, auquel cas la voie du recours n'est pas ouverte contre une telle décision[591].

578 Ce dernier constat est choquant, car même si l'appel est ouvert contre cette décision intermédiaire en même temps que la décision finale, il ne reste pas moins qu'il existe une divergence notable entre la situation d'un individu qui se voit prélever ses empreintes en urgence durant la procédure de première instance et celui dont la saisie de données signalétiques est ordonnée par le ministère public ou la police. En outre, nous comprenons difficilement pourquoi il faudrait attendre le jugement final pour attaquer la décision sur la saisie des données signalétiques qui n'est pas de nature à influencer le jugement au fond[592]. C'est pourquoi, comme le relèvent André Kuhn et Camille Perrier[593], il est préférable de

[586] BSK-StPO-WERLEN, art. 260 N 4-5; MULLIS, p. 312; StPO-HANSJAKOB, art. 260 N 10.

[587] Message, CPP, p. 1225.

[588] SCHMID, Praxiskommentar, art. 260 N 13; StPO-HANSJAKOB, art. 260 N 13.

[589] CR-CPP-RÉMY, art. 393 N 11; SCHMID, Praxiskommentar, art. 393 N 9; StPO-KELLER, art. 393 N 15, 21 et 27.

[590] Message, CPP, p. 1296.

[591] SCHMID, Praxiskommentar, art. 65 N 1; StPO-BRÜSCHWEILER, art. 65 N 1; StPO-KELLER, art. 393 N 27-28.

[592] Message, CPP, p. 1296.

[593] KUHN, PERRIER, N 18.

considérer une mesure de contrainte prise en urgence à une décision du tribunal afin d'éviter que le magistrat ne puisse soustraire sa décision à la voie du recours.

ii. L'enregistrement dans AFIS

579 Si la saisie des empreintes papillaires n'atteint que légèrement aux droits fondamentaux de la personne concernée par la mesure coercitive, l'utilisation et la conservation de ces données signalétiques peuvent avoir des conséquences plus lourdes.

580 L'intérêt de l'Etat à compléter la base de données AFIS pour qu'elle soit la plus exhaustive et efficace possible s'oppose à l'intérêt de chaque individu à son droit à l'autodétermination informationnelle (art. 13 al. 2 Cst).

581 L'art. 261 CPP règlemente notamment l'utilisation des données signalétiques qui ne se trouvent pas dans le dossier de procédure (art. 100 *a contrario* CPP). Cet article est complété par l'ordonnance sur le traitement des données signalétiques.

a) Le traitement des empreintes digitales et palmaires

582 L'exploitation des données signalétiques débute par le traitement de la donnée – dans notre hypothèse de travail de l'empreinte digitales ou palmaire – dans le système automatisé AFIS géré par la Fedpol (art. 1 al. 1 AFIS-O). L'intégration d'une empreinte papillaire permet d'exploiter de manière centralisée la donnée afin d'identifier un individu ou d'établir un lien entre plusieurs infractions (art. 1 al. 2 et 3 let. a AFIS-O).

583 Diverses autorités listées à l'art. 4 AFIS-O, dont notamment la police judiciaire fédérale et les services d'identification compétents des autorités de police cantonales, peuvent demander au service AFIS ADN d'effectuer une comparaison des empreintes digitales, des empreintes palmaires et des traces relevées sur une scène de crime.

584 Une fois la saisie des empreintes effectuée, celles-ci sont intégrées au fichier AFIS qui comprend quatre catégories de données: les empreintes des deux doigts, les empreintes des dix doigts, les empreintes palmaires et les traces relevées (art. 7 al. 1 AFIS-O). Complétées avec des informations sur le dessin papillaire, les données saisies sont mises en mémoire dans AFIS.

585 Outre les informations sur les lieux du délit, aucune autre information personnelle n'est détenue dans AFIS. En effet, chaque empreinte enregistrée contient un numéro de contrôle du processus qui n'est relié au fichier IPAS[594], AUPER[595] ou avec le RCE[596] que si une concordance a été retenue par les experts. Ce n'est d'ailleurs que dans cette dernière hypothèse que le service AFIS-ADN transmet les données personnelles – nom, prénom, date de naissance, etc. (art. 16 al. 1 AFIS-O) – à l'autorité ayant demandé la comparaison.

b) L'utilisation des données enregistrées dans AFIS

586 La saisie de l'empreinte papillaire est bien entendu utile dans le cadre d'une procédure pendante durant laquelle la mesure de contrainte a été ordonnée. En outre, une donnée signalétique peut être utilisée en dehors du dossier de procédure lorsque des soupçons suffisants laissent présumer une récidive (art. 261 al. 1 CPP).

587 L'intérêt de l'Etat est de pouvoir disposer de certaines données quand une récidive s'avère probable afin d'assurer la sécurité publique et une bonne administration de la justice. Il peut donc s'avérer nécessaire d'utiliser hors dossier de procédure des empreintes papillaires préalablement enregistrées afin d'identifier un individu ou de lier les scènes de crime entre elles.

588 Les empreintes étant utilisées en dehors du but ayant déterminé leur saisie, la notion de "*soupçons suffisants*" doit être interprétée de manière restrictive[597]. Employée trop largement, une atteinte importante aux droits fondamentaux de l'individu concerné serait causée.

589 Par conséquent, lorsqu'une empreinte ou toute autre donnée signalétique est employée hors dossier de la procédure, il est impératif de respecter le principe de proportionnalité de façon stricte. Il est nécessaire que les soupçons de récidive ne soient pas seulement "*suffisants*", mais qu'ils soient avérés et élevés, voire que la gravité de l'infraction soit prise en considération.

[594] L'IPAS est le fichier de gestion et d'indexation de dossiers et de personnes géré par la Fedpol. Infra Partie II, Chapitre 3, III, B, 2, c, n° 2218 ss.

[595] L'AUPER est le système d'enregistrement automatisé des personnes.

[596] Le RCE est le registre central des étrangers.

[597] CR-CPP-ROHMER, art. 261 N 9; StPO-HANSJAKOB, art. 261 N 8.

iii. La conservation et la destruction d'une fiche signalétique dans AFIS

590 La jurisprudence concordante du Tribunal fédéral et de la Cour européenne des droits de l'homme reconnaît que les données stockées dans un système informatisé, tel que le fichier AFIS, ne peuvent l'être *ad vitam aeternam*[598].

591 Une pesée des intérêts doit être effectuée entre l'intérêt de l'Etat à disposer d'archives pour effectuer des recoupements futurs et l'intérêt des individus à obtenir l'effacement de leurs données personnelles.

a) La conservation des données signalétiques au sens de l'art. 261 CPP

592 L'art. 261 CPP règlemente selon les circonstances la durée de conservation des données signalétiques, extensivement des empreintes digitales.

593 Lorsque la personne concernée par la saisie des empreintes digitales ou palmaires est le prévenu et qu'il a été condamné ou acquitté pour cause d'irresponsabilité, ses données lophoscopiques sont conservées jusqu'à l'expiration des délais impartis pour la radiation des inscriptions au casier judiciaire (art. 369 CP *cum* art. 261 al. 1 let. a CPP).

594 En cas d'acquittement, de classement de procédure (art. 320 al. 4 CPP prévoit expressément qu'un classement équivaut à un acquittement) ou d'ordonnance de non-entrée en matière[599], les données sont radiées immédiatement à l'entrée en force du jugement (art. 261 al. 1 let. b CPP). Cependant, si les données lophoscopiques peuvent – avec une certaine probabilité – être utilisées pour identifier l'auteur d'infractions futures, elles sont conservées et utilisables pendant dix ans à compter de l'entrée en force de la décision.

595 Quant aux empreintes d'une personne qui n'a pas la qualité de prévenu, ses données automatisées sont détruites immédiatement après la clôture de la procédure contre le prévenu (art. 261 al. 3 CPP).

596 Les données devenues inutiles, comme moyen de preuve ou parce que l'accusé est décédé (art. 17 al. 1 AFIS-O) sont détruites immédiatement (art. 261 al. 4 CPP). L'intérêt public nécessaire à la restriction des droits fondamentaux n'étant plus donné, la conservation

[598] ATF 109 Ia 146, 155-157; ATF 120 Ia 147, 151 = JdT 1996 IV 61, 61; CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 119-125

[599] ATF 109 Ia 146, 157; ATF 113 Ia 257, 263; De 29 à l'unité, p. 194; HAUSER, SCHWERI, HARTMANN, p. 373.

violerait illicitement la sphère privée des individus (art. 8 al. 2 CEDH, art. 17 § 1 Pacte II et 13 al. 2 Cst).

b) La conservation des données selon l'Ordonnance réglementant l'AFIS

597 En comparant l'Ordonnance réglementant l'AFIS, soit l'ordonnance sur le traitement des données signalétiques biométriques (Ordonnance sur les données signalétiques), avec le Code de procédure pénale, des précisions mais aussi des divergences apparaissent relativement aux durées de conservation.

598 Les empreintes digitales des personnes ne pouvant pas être l'auteur du délit ou les traces s'avérant être attribuables à une personne ne pouvant pas être l'auteur de l'infraction (art. 17 al. 1 let. a AFIS-O) doivent être effacées immédiatement. Lorsque ni demande, ni décès n'intervient, l'effacement a lieu au plus tard trente ans après le traitement signalétique (art. 17 al. 3 let. a AFIS-O). A noter que le suspect s'avérant ne pas être l'auteur de l'infraction considérée ne peut pas demander lui-même l'effacement de ses données (art. 22 *a contrario* AFIS-O).

599 En fin de compte, l'art. 17 AFIS-O complète et précise les cas où l'intérêt public fait défaut et donc que la destruction des données s'impose. Ainsi, l'applicabilité de cette disposition n'est pas remise en cause par l'édiction de l'art. 261 al. 4 CPP.

600 L'application de l'art. 17 AFIS-O relatif à la destruction des empreintes papillaires dans le secteur policier est plus problématique depuis la mise en vigueur du Code de procédure pénale fédéral.

601 L'effacement des données est immédiat en cas d'acquittement ayant force de droit (art. 17 al. 1 let. c AFIS-O), sauf si la décision est rendue pour cause d'irresponsabilité de l'auteur (art. 17 al. 2 AFIS-O); lorsque la peine prononcée est assortie du sursis, les empreintes sont supprimées cinq ans après la fin du délai d'épreuve (art. 17 al. 1 let. e AFIS-O); la durée de cinq ans est également instaurée pour l'effacement après le paiement d'une peine pécuniaire ou l'exécution d'un travail d'intérêt général (art. 17 al. 1 let. f AFIS-O); finalement, le service AFIS ADN efface les empreintes digitales ou palmaires vingt ans après la libération suite à une peine privative de liberté, d'un internement, ou après l'exécution d'une mesure thérapeutique (art. 17 al. 4 AFIS-O). De surcroît, l'autorité compétente peut refuser la destruction des données, si une enquête en cours existe ou s'il est à craindre que l'auteur récidive (art. 19 AFIS-O).

602 Même s'il est exact que les art. 17 al. 2 AFIS-O et 261 al. 2 CPP présentent de fortes similitudes pouvant coexister, tel n'est pas le cas des art. 17 al. 1 AFIS-O et 369 CP *via* 261 al. 1 let. a CPP.

603 Les durées de conservation du casier judiciaire diffèrent sensiblement de celles prévues dans l'ordonnance du 6 décembre 2013. La conservation durant vingt années n'est possible que pour les peines privatives de liberté d'au moins cinq ans (369 al. 1 let. a CP), elle n'est que de quinze ans pour les peines privatives de liberté de un à moins de cinq ans, et de dix ans pour celles de moins d'un an. Lorsqu'une peine privative de liberté avec sursis, une peine pécuniaire, un travail d'intérêt général ou une amende est prononcé, les données sont conservées durant dix ans (art. 369 al. 3 CP), et pas seulement cinq (art. 17 al. 1 let. e et f AFIS-O). Si une mesure thérapeutique ou un internement est décidé, l'effacement intervient après quinze ans (art. 369 al. 4 let. a CP).

604 Au vu des divergences importantes et inconciliables entre les dispositions de AFIS-O et celle du Code de procédure pénale qui renvoie au Code pénal, la question se pose de savoir quelles sont les durées applicables à l'élimination des fiches décadactylaires ou monodactylaires de la base de données AFIS. A ce sujet, les dispositions du CPP et le message du Conseil fédéral sont silencieux, aucune modification ou abrogation de l'art. 16 aAFIS-O n'est mentionnée, remplacé par l'art. 17 AFIS-O, et les auteurs des commentaires sur le Code de procédure pénale éludent la problématique de la coexistence de la base légale de l'ordonnance et de l'art. 261 al. 1 let. a CPP[600]. Seule la Chancellerie fédérale répond à ce sujet que, de manière générale, lorsqu'une situation comme celle-ci existe "*il paraît évidant qu'à la prochaine modification de loi une abrogation ou modification sera effectuée*"[601], si tant est qu'il n'y ait pas d'oubli, ce qui nuit, dans l'intervalle, à la sécurité juridique. D'ailleurs, force est de constater que l'entrée en vigueur de AFIS-O n'a pas réglé toutes les divergences qui existaient du temps de l'ancienne AFIS-O.

605 Plus problématique est le fait que même si le Code de procédure pénale prévaut quant à sa supériorité hiérarchique et à sa pertinence, l'Ordonnance sur les données signalétiques est postérieure si bien qu'on ignore quelles dispositions prédominent.

---

[600] A ce sujet: GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 246; JOSITSCH, Strafprozessrechts, p. 139; PERRIER, VUILLE, p. 155; Polizeiliche Ermittlung-ALBERTINI, SCOSSA-BAGGI, p. 405; SCHMID, Praxiskommentar, art. 261 N 1 ss; StPO-HANSJAKOB, art. 261 N 1 et 12.

[601] Information obtenue par le Centre des publications officielles du Secteur Conseil fédéral de la Chancellerie fédérale.

606 Cela étant, il paraît par ailleurs inexact de prétendre que les art. 17 ss AFIS-O seraient une *lex specialis* par rapport à l'art. 261 CPP, puisque ce dernier affirme clairement réglementer non pas la radiation des casiers judiciaires, mais bien celle des données signalétiques. De plus, le renvoi à l'art. 369 CP a l'avantage de régler l'effacement des données de manière plus précise, tant en ce qui concerne les empreintes d'une personne condamnée à une peine privative de liberté – une différenciation étant faite en vertu de la durée de la peine –, que celle découlant de la prise d'empreintes d'une personne sanctionnée par un traitement ambulatoire ou une autre mesure des art. 66 à 67*b* CP.

607 En conséquence, à notre avis, les art. 17 ss AFIS-O perdent de leur essence et il est nécessaire d'appliquer le dispositif légal en vigueur selon le Code de procédure pénale. En revanche, l'ordonnance dans son entier ne doit pas être considérée comme désuète. Bien au contraire, elle encadre la procédure de traitement et de communication des résultats et précise certains points où le CPP reste muet.

c) La destruction des données signalétiques

608 Dans les cas visés par l'art. 261 al. 1 à 3 CPP et à l'échéance des délais, les données doivent être détruites. Cette obligation prévaut également pour la radiation des données signalétiques au sens de l'Ordonnance AFIS. Au surplus, pour respecter au mieux les délais de conservation et éviter une atteinte non justifiée aux droits fondamentaux des personnes concernées, il serait préférable d'instaurer une destruction automatique des données plutôt qu'un effacement sur demande.

609 Quant aux données prévues par l'art. 261 al. 4 CPP, elles sont effacées d'office[602] et nonobstant l'écoulement d'un délai puisque c'est leur nature même de données inutiles qui fonde la radiation.

2. L'identification judiciaire et la preuve dactyloscopique

610 Depuis plusieurs décennies[603], les empreintes digitales sont des indices matériels importants dans le procès pénal. Leur fréquence d'exploitation judiciaire équivaut à celle de toutes les autres techniques de police scientifique réunies[604].

[602] StPO-HANSJAKOB, art. 261 N 12.

[603] Supra Partie I, Chapitre 1, II, B, 1, b, n° 72 ss.

[604] Information disponible sur le site internet d'Interpol: http://www.interpol.int [consulté le 08.05.2016].

611 Permettant diverses comparaisons, extensivement l'élucidation de faits importants aux affaires pénales, l'apport des empreintes digitales ou palmaires en Suisse n'est plus à prouver. Une comparaison entre une empreinte déposée sur les lieux de l'infraction ou sur un objet lié à celle-ci avec une empreinte fichée et/ou connue permet d'apporter devant la Cour un élément de preuve – plus ou moins infaillible – de l'identité de l'auteur.

612 Du fait de son objectivité et de sa valeur scientifique, la preuve dactyloscopique est largement appréciée, mais l'identification d'un individu dans le procès pénal reste une décision judiciaire dont le fardeau revient à la Cour et non au criminaliste. Il est essentiel que le juge puisse appréhender correctement le résultat identificatoire rendu par l'expert, déterminer ce qu'il démontre objectivement et quelle en est la force probante.

a. La nature déterministe de l'identification

i. L'absence de consensus international et les résolutions de l'association professionnelle internationale pour l'identification (IAI)

613 La pratique internationale concernant la preuve identificatoire dactyloscopique n'est pas uniformisée[605]. Certains Etats exigent un nombre minimal de minuties pour reconnaître une identification formelle – en Grande-Bretagne, le chiffre minimal est de seize points caractéristiques, limite pouvant être abaissée à quatorze minuties similaires, selon la gravité de l'infraction; en France, Belgique, Portugal, Espagne et bien d'autres Etats, le nombre minimum est de douze – ou fixent un intervalle – selon l'usage, l'Allemagne, la Suède et la Hollande fixent un intervalle entre huit et douze minuties – dont la limite inférieure est suffisante si des particularités existent. Alors que pour d'autres aucun *minima* n'est prévu, l'identification étant uniquement une question de jugement.

614 Le manque de consensus international pour déterminer la force probatoire de l'identification dactyloscopique met à mal la valeur scientifique de cette preuve. Pour tenter de pallier les divergences et les doutes subséquents, des résolutions destinées aux professionnels des sciences forensiques ont été formulées par l''International Association for Identification (IAI). D'après leurs constatations, il n'existe pas d'élément probant pour justifier la fixation d'un standard minimum[606]. La nature même de l'unicité des empreintes digitales par les diverses

[605] A ce sujet: CHAMPOD, Friction Ridge Skin, p. 111 ss; CHAMPOD, Reconnaissance, p. 2-3; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 28.

[606] ANONYME, International Association for Identification: standardization committe report, in *FBI Law Enforcement Bulletin* 42 (1973), p. 8.

minuties impose la proscription d'une norme numérique[607]. Néanmoins, un standard minimum peut éviter les erreurs crasses, principalement lors d'analyses effectuées par des dactyloscopes inexpérimentés.

615 En 1980[608], l'IAI a en outre fixé une ligne directrice interdisant aux experts d'apporter une réponse complétée par un qualificatif, tel que "possible", "probable", "très probable", "peu probable", etc. Corrélativement à la volonté de la majorité des experts dactyloscopes, la preuve dactyloscopique ne devrait jamais être présentée par un avis qualifié, la probabilité d'erreur lors de spéculation ne pouvant être connue.

616 Les résolutions de l'IAI n'ayant aucune force juridique[609], les pays restent toutefois libres d'instaurer leur propre réglementation pour déterminer si oui ou non l'identification dactyloscopique est viable et probante.

ii. L'identification dactyloscopique en Suisse

617 Jusqu'en 2007, les experts suisses favorisaient l'approche quantitative en retenant qu'une concordance entre huit à douze points rendait l'identification certaine, étant précisé que le rapport identificatoire était exclusivement fourni au juge lorsque douze minuties étaient relevées et similaires[610]. Dès le mois de novembre 2007, les chefs de la division AFIS ont décidé de passer à l'approche holistique[611].

618 Partant du postulat que l'individualisation d'une empreinte ne peut pas se réduire à compter le nombre de minuties similaires[612], l'approche holistique ou non-numérique met en balance

---

607 ANONYME, International Association for Identification: standardization committe report, in *FBI Law Enforcement Bulletin* 42 (1973), p. 8; CHAMPOD, Fingerprint, p. 7; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; MARGOT, CHAMPOD, p. 233.

608 INTERNATIONAL ASSOCIATION FOR IDENTIFICATION, Resolution VII amended, in *Identification News* 30 (1980), p. 3.

609 INTERNATIONAL ASSOCIATION FOR IDENTIFICATION, Resolution VII amended: "*THEREFORE BE IT RESOLVED that any member, officer or certified latent print examiner who provides oral or written reports, or gives testimony of possible, (underlined for emphasis) probable or likely friction ridge identification shall be deemed to be engaged in conduct unbecoming such member, officer or certified latent print examiner as described in Article XVII, Section 5, of the constitution of the International Association for Identification, and charges may be brought under such conditions set forth in Article XVI, Section 5, of the constitution. If such member be a certified latent print examiner, his conduct and status shall be reconsidered by the Latent Print Certification Board...*".

610 CHAMPOD, Reconnaissance, p. 15; PFEFFERLI, p. 220.

611 Information obtenue de Monsieur Axel GLAESER, Chef de division du service AFIS ADN.

612 CHAMPOD, Fingerprint, p. 7; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; INTERNATIONAL ASSOCIATION FOR IDENTIFICATION, Standardization Committee report, in *FBI Law Enfoncement Bulletin* 42 (1973), p. 7-8.

l'aspect quantitatif – avec le nombre de minuties – et qualitatif – avec la forme générale des lignes papillaires, des pores, de leur combinaison ou du type de minuties – des points visibles sur le dessin de l'empreinte[613].

619 La nécessité d'appréhender les circonstances du dépôt et la qualité des concordances lorsque moins de douze minuties similaires sont découvertes a nécessité le classement des experts en trois niveaux de compétences.

620 En cas d'empreintes complexes – contenant moins de douze minuties –, les années de pratiques sont un atout pour l'expert qui est à même de déterminer la fréquence ou l'exceptionnalité d'une minutie précise. Ainsi, une telle approche permet de reconnaître un potentiel identificatoire similaire entre six minuties exceptionnelles et douze minuties communes analysées respectivement par un expert expérimenté et débutant, et donc d'augmenter la fréquence des identifications formelles.

621 Quant aux conclusions identificatoires, en s'appuyant sur la caractéristique d'unicité des empreintes papillaires et en niant les probabilités qui affirmeraient que plusieurs donneurs potentiels existent, les dactyloscopes suisses ont opté pour la nature déterministe de l'identification.

622 Les conclusions du processus de comparaison sont de cinq ordres: l'empreinte analysée est identifiable et identifiée; l'empreinte examinée n'ayant pas assez de points caractéristiques ne peut pas fournir un résultat positif; l'empreinte n'est pas directement exploitable pour fournir l'identité de l'auteur, cependant des points distinctifs sont suffisants pour exclure avec certitude des personnes déterminées; l'empreinte fournit trop peu d'informations, mais si des concordances existent, que la police suspecte fortement une personne et que l'expert connaît les doutes de la police, il est en droit de répondre : "*Il n'est pas à exclure que la personne faisant l'objet de l'enquête soit l'auteur de la trace latente examinée*", sans autres précisions; l'empreinte de référence est de mauvaise qualité et ne permet aucune analyse.

623 En définitive, la preuve dactyloscopique est une preuve dichotomique ne laissant place à aucune interprétation ou spéculation[614].

---

[613] ASHBAUGH, p. 6; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 30; PFEFFERLI, p. 220.

[614] CHAMPOD, Reconnaissance, p. 3; CHAMPOD, LENNARD, MARGOT, STOILOVIC, p. 33; MARGOT, CHAMPOD, p. 236.

b. La valeur probatoire

i. La valeur probatoire scientifique reconnue

624 L'intégration de la science dans le cadre juridique n'est pas dénuée de tout fondement. Elle assiste la justice pour atteindre son objectif lié à la recherche des éléments nécessaires pour fonder un jugement de condamnation ou d'innocence, soit à la punition des actes délictueux. Dans ce sens, la dactyloscopie est une méthode fiable, généralisable, rapide et peu coûteuse pour tenter d'identifier l'auteur d'un acte criminel et constituer des archives pour confondre les récidivistes[615].

625 Pour établir l'identité d'une personne directement ou indirectement concernée par la perpétration d'une infraction, nous l'avons vu, un processus scientifique est obligatoire[616]. Une fois réalisé et lorsqu'un hit est détecté[617], le service AFIS ADN transmet par le biais d'une plateforme sécurisée un message à l'autorité chargée de l'enquête et à l'origine de la demande de comparaison. Reposant sur le postulat déclarant que les dessins papillaires sont individualisés et sur plus de cent années d'expériences durant lesquelles peu d'erreurs ont été décelées, les dactyloscopes déclarent que les empreintes digitales sont un moyen d'identification fiable et incontestable dès lors que rien ni personne n'a pu démontrer qu'ils avaient tort de penser ainsi[618]. Cela étant, certains experts forensiques préconisent de dire que l'empreinte digitale ne permet pas d'identification, mais une présomption[619].

626 Peu importe que le fichage d'une empreinte date d'une année, de dix ans ou plus, ou qu'elle soit endommagée, la comparaison et l'identification restent possibles. Un récidiviste ou toute personne ayant fait l'objet d'un profilage de ses empreintes ne peut donc pas arguer une modification des dessins papillaires pour nier l'identification effectuée par la méthode lophoscopique, à moins qu'un jour l'un d'eux entreprenne la monumentale opération qui consiste à retirer l'entièreté des téguments composés de crêtes épidermiques et à greffer une nouvelle peau. De plus, grâce au processus aléatoire de la morphogénèse durant la gestation, même les jumeaux univitellins ont des empreintes papillaires différentes, alors même que leur patrimoine ADN est identique.

---

615 CHAMPOD, Reconnaissance, p. 3 et 268; LE DOUARIN, p. 2.

616 Supra Partie II, Chapitre 2, I, A, 2, n° 530 ss.

617 Supra Partie II, Chapitre II, I, A, 2, c, i, n° 544 ss.

618 CHAMPOD, Reconnaissance, p. 268; LE DOUARIN, p. 2.

619 CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; NATIONAL RESEARCH COUNCIL, p. 109.

627 Scientifiquement, la valeur probatoire des empreintes digitales est donc absolue et sans restriction. Néanmoins, le résultat identificatoire n'est pas une décision, mais uniquement une proposition transmise à la justice après validation par l'office de police cantonale ou toute autre autorité à l'origine de la demande. En aucun cas l'examinateur scientifique, extensivement le service AFIS ADN, n'a les capacités d'imposer son avis à l'autorité policière et judicaire.

628 Le principe de la libre appréciation des preuves dominant le procès pénal[620], en théorie, les empreintes digitales comme moyen identificatoire n'ont pas une force probatoire déterminée. Par conséquent, la valeur scientifique ne s'impose pas dans le cadre procédural et le juge est en droit de la réfuter par des considérants juridiques. Les juges de fond sont donc aptes à déterminer les éléments probatoires nécessaires pour forger leur intime conviction. Ils ont également la difficile tâche d'évaluer la valeur probante, la crédibilité et la suffisance d'un élément de preuve.

629 La pratique judiciaire démontre toutefois que la preuve dactyloscopique joue un rôle décisif dans l'identification d'une personne. Quand bien même un accusé clame que l'empreinte trouvée sur les lieux du crime ne lui appartient pas personne ne le croit[621], principalement parce que le juge estime que la science prouve le contraire et qu'il craint – parfois à tort – de s'écarter des considérants scientifiques. Au gré des évolutions, l'évaluation de la preuve dactyloscopique se complexifie creusant exponentiellement le fossé entre les aptitudes des juristes et celles des dactyloscopes. Bien souvent, les magistrats suivent les déclarations de l'expert sans débattre sur la valeur probatoire faute d'avoir les compétences pour ce faire.

630 Il est certain que si un "hit" est obtenu à l'aide d'une empreinte claire, précise et de qualité excellente, la discussion quant à la certitude scientifique est inutile, puisqu'il est largement reconnu que deux individus ne peuvent avoir la même empreinte. Tel n'est en revanche pas le cas lorsqu'une empreinte est de mauvaise qualité ou contient peu de minuties.

631 Cependant, il ne faut pas en conclure que, juridiquement, l'identification grâce aux empreintes papillaires n'a pas de force probante autonome. Les tribunaux apprécient tout de même selon leur capacité la preuve dactyloscopique.

---

[620] Supra Partie I, Chapitre 3, III, C, n° 313 ss.

[621] GYSIN, p. 12.

ii. La preuve dactyloscopique et le faisceau d'indices

632 Dans une affaire datant de 2005[622], des traces papillaires ont été examinées sans succès identificatoire. Le recourant reproche à l'autorité cantonale de jugement de ne pas avoir pris en considération ces empreintes non-attribuées pour rendre sa décision. Le Tribunal fédéral relève que, comme le permet son pouvoir d'appréciation, la Cour apprécie la preuve dactyloscopique de manière objective et spatiale. Les traces papillaires ayant été détectées dans des parties communes d'une entreprise ainsi que dans un bureau grandement fréquenté durant la journée, les empreintes peuvent appartenir soit à l'auteur, soit à un innocent, et ne permettent pas de mettre en doute la culpabilité du recourant. Certes, le Tribunal fédéral ne discute pas du processus d'identification, soit de la phase scientifique, ni même des résultats non-déterminants de l'expert dactyloscope, ou encore de savoir si la comparaison a été effectuée dans les règles de l'art, mais ces questions peuvent rester ouvertes, puisque, prises isolément, de telles empreintes ne prouvent rien ni à charge ni à décharge.

633 Conséquemment, une empreinte déposée et identifiée, appréciée séparément des autres indices ou preuves n'est juridiquement pas probante. La trace papillaire est une simple preuve de contact entre une personne et un objet ou une surface liée à une infraction[623]. Ainsi, elle doit s'intégrer dans un faisceau d'indices concourant à la décision d'identification[624], sans quoi l'intime conviction obtenue serait entachée d'arbitraire. Il n'est en revanche pas nécessaire de recourir à un autre moyen de preuve pour reconnaître le faisceau d'indices.

634 En 2006, un grief est porté devant le Tribunal fédéral[625] dans une affaire de vol d'une bourse dans un véhicule stationné dont la vitre conducteur était légèrement ouverte. Le recourant reprochait à la Cour cantonale de s'être appuyée uniquement sur la présence de ses empreintes sur la vitre du véhicule pour admettre un verdict de culpabilité. A cet égard, les juges fédéraux rappellent qu'il n'est pas arbitraire de juger coupable un individu en s'appuyant sur la présence de ses empreintes digitales. *In casu*, la Cour cantonale s'est certes basée sur l'identification des empreintes papillaires, mais ce qui a été déterminant était l'emplacement desdites empreintes qui se trouvaient sur la face extérieure et surtout intérieure de la vitre, ainsi que le manque d'explications crédibles du recourant[626]. Le

[622] TF 6P.47/2005 du 30 mai 2005, c. 3.5.

[623] CHAMPOD, Overview, p. 308; MARGOT, LENNARD, Empreintes, p. 13; WALDER, p. 41.

[624] CHAMPOD, Reconnaissance, p. 17; PFEFFERLI, p. 221.

[625] TF 1P.822/2005 du 4 juillet 2006.

[626] TF 1P.822/2005 du 4 juillet 2006, c. 3.2.

Tribunal fédéral a donc tranché la problématique grâce à une évaluation globale des circonstances, soit à l'aide de la preuve dactyloscopique et des éléments obtenus grâce à elle. Dans de telles circonstances, il serait en outre préférable que la justice s'intéresse de plus près à la qualité de l'empreinte, aux qualifications de l'expert et au cheminement qui ont mené ce dernier à rendre un résultat identificatoire positif, afin de juger correctement et complètement de la valeur de la preuve dactyloscopique apportée.

635 En conséquence, la preuve dactyloscopie ne doit être qu'une aide à forger l'intime conviction du juge grâce à ses qualités scientifiques, mais ne doit en aucun cas être considérée comme une preuve de culpabilité.

C. La discussion sur la preuve dactyloscopique

636 Une enquête américaine[627] a conclu que 85% des 978 jurés auditionnés considèrent la preuve dactyloscopique comme la méthode la plus fiable d'identification.

637 L'acceptation dans le monde judiciaire suisse n'a pas fait l'objet d'une enquête précise, mais il paraît vraisemblable que les empreintes digitales ne sont pas sans influence au cours des procès.

638 Cependant, la fragilité de la science et de la pratique à la base de l'identification – le risque d'erreur, les inconvénients liés aux résultats identificatoires, l'usage d'un traitement automatisé ou l'atteinte aux droits fondamentaux – ne sont pas à négliger, tout comme les nombreux avantages de cette méthode identificatoire

1. L'évaluation de la preuve dactyloscopique dans l'ordre judiciaire suisse

a. Le potentiel de la preuve dactyloscopique

i. Une preuve hybride

639 La preuve dactyloscopique est incontestablement une preuve hybride. Elle se compose d'une empreinte digitale, soit d'une trace indiciale matérielle qui est détectée et constatée

[627] BECUE, CHAMPOD, EGLI, MORET, p. 4; EPSTEIN Robert, Fingerprints meet Daubert: The Myth of Fingerprint "Science" is revealed, in *California Law Review* 75 (2002), p. 605-657, 605.

directement sur les lieux de l'infraction ou sur un objet s'y trouvant, ainsi que d'une inférence[628].

640 Conséquemment, le juge ne saisit pas directement la portée de l'indice en présence. Un raisonnement/une interprétation est nécessaire. Cet aspect subjectif peut rendre l'empreinte papillaire plus facilement contestable qu'une preuve purement matérielle, c'est pourquoi il est contrebalancé par l'objectivité de la science et de l'expert.

641 L'expert n'étant pas partie au procès et ne déclarant pas ce qu'il a vu ou entendu, mais uniquement ce qui résulte du processus identificatoire scientifique, ses conclusions sont plus fiables que celles d'un témoin; d'autant que le scientifique agit conformément à la déontologie en faisant honneur à sa profession et en agissant en toute impartialité[629]. En cas de doute quant à l'objectivité de l'expertise, il est toujours possible d'interroger le professionnel ou de recourir à une contre-expertise pour s'assurer de la bonne application des principes scientifiques.

642 Mi-subjectives, mi-objectives, les traces papillaires ont pour les criminalistes le pouvoir de faire avancer l'enquête. Sans cette science, bon nombre d'affaires criminelles n'auraient pas été résolues à défaut de connaître l'identité du potentiel coupable.

643 L'atout majeur de la preuve dactyloscopique est donc son caractère scientifique qui permet de prouver, d'argumenter ou de motiver les résultats identificatoires, extensivement d'accorder un certain poids aux dires de l'expert. La dactyloscopie procure une certitude d'ordre physique[630] préférable aux présomptions morales qui peuvent entacher les preuves testimoniales.

ii. La reconnaissance scientifique

644 La forte reconnaissance scientifique de l'apport des empreintes papillaires et leurs triples caractéristiques font l'objet d'une exégèse développée. Nous nous bornerons donc à affirmer que ces deux points fondent les qualités et l'intérêt positif de l'empreinte papillaire comme moyen de preuve sans intégrer de développements conséquents.

---

[628] GALLUSER, p. 8; PIQUEREZ, Traité de procédure pénale suisse, p. 380.

[629] CHAMPOD, VUILLE, p. 30; VUILLE, Thèse, p. 356-360.

[630] CHAMPOD, Reconnaissance, p. 268; LE DOUARIN, p. 2; LOCARD, T. I-II, p. 226.

645 La conviction des experts et des juristes concernant la fiabilité de la preuve dactyloscopique repose principalement sur la qualité de loi physique et scientifique. Une telle loi vaut par elle-même. Elle ne nécessite aucune application ou concrétisation. Elle n'a pas à être interprétée et ne peut pas être erronée. Elle existe parce que le monde existe. Elle n'est pas créée ni transformée par les dactyloscopes.

646 Scientifiquement, si le processus d'identification est réalisé dans les règles de l'art, sans subjectivité, en suivant à la lettre les principes dactyloscopiques, ainsi que les prérogatives devant être remplies pour exploiter correctement une trace indiciale, aucune erreur de droit imputable à l'empreinte papillaire n'est possible[631]. Le risque n'est lié qu'à l'interprétation des magistrats lorsqu'une identification est réalisée et présentée au procès, ou – éventuellement – au travail peu satisfaisant du dactyloscope généralement lié à la mauvaise qualité d'une empreinte ou à sa subjectivité qui ne devrait pas exister.

647 Le peu d'erreurs identificatoires documentées jusqu'à aujourd'hui permet d'affirmer que ce moyen de preuve n'est pas illusoire et a acquis avec les années une valeur inestimable aux yeux des juristes. La pratique démontre qu'implicitement la force théorique et objective des empreintes digitales comme moyen de preuve est grandement prise en considération lors de l'appréciation des preuves par le magistrat sans grand débat[632].

648 L'importance de la valeur scientifique et sa reconnaissance dans le temps doivent tout de même être nuancées. Certaines techniques sont exploitées depuis de nombreuses années, alors que d'autres ont fait leur apparition plus ou moins récemment. Vraisemblablement, avec l'évolution perpétuelle de la science, de la physique et de la chimie, l'exploitation de techniques inconnues encore aujourd'hui n'est pas à écarter. Dès lors, il peut être erroné d'affirmer que la valeur scientifique de la dactyloscopie repose sur plusieurs dizaines d'années. Certes, les trois prémisses que sont l'individualité, la pérennité et l'inaltérabilité, ainsi que l'importance des minuties datent et sont ancrées dans la pratique depuis longtemps, mais la détection des empreintes dermatoglyphes permettant d'obtenir un dessin papillaire analysable avec plus ou moins de clarté peut résulter d'une technique récente.

649 La qualité de la trace indiciale influençant sur le résultat identificatoire, il nous paraît important de tenir compte de la méthode de détection utilisée lors de l'appréciation de la preuve dactyloscopique. Ainsi, une technique récente ayant moins d'assise, la valeur

---

631 GYSIN, p. 12.

632 TF 6P.47/2005 du 30 mai 2005, c. 3.1. Par analogie pour la preuve pénale: RR.2007.173, c. 4.3; RR.2008.47, c. 2.2; E-2565/2010. A ce sujet, voir: CHAMPOD, TARONI, RPS 1993, p. 224.

scientifique et le pouvoir probatoire de l'identification y afférant doivent être nuancés en conséquence comparativement à une technique ayant fait ses preuves.

iii. Les facultés probatoires à charge ou à décharge

650 Lorsqu'une personne est suspectée, que de forts soupçons pèsent sur elle et que le processus identificatoire fournit une correspondance certaine entre l'empreinte indiciale et son empreinte dermatoglyphe, la preuve dactyloscopique est une preuve utilisable à charge. Elle permet de prouver l'identité de l'auteur ou – tout du moins – la présence de l'individu identifié sur les lieux de l'infraction, voire le contact entre cette personne et un objet lié à l'acte délictuel.

651 En revanche, si des traces papillaires sont retrouvées sur le corps de la victime, sur l'arme du crime et à divers endroits stratégiques de la scène de crime, qu'une comparaison est effectuée avec les empreintes du suspect, mais que la conclusion du dactyloscope énonce des dissemblances, alors la preuve dactyloscopique permet d'innocenter le suspect.

652 De même, si une trace digitale est révélée sur l'arme du crime, qu'aucun autre indice ne permet d'identifier le coupable, et qu'après confrontation, il n'est pas possible d'identifier l'accusé comme l'auteur du crime, il est possible d'administrer la preuve dactyloscopique pour faire planer le doute sur l'implication du suspect, voire du prévenu. Le doute profitant à l'accusé, le juge du fond ne peut que reconnaître l'accusé innocent.

653 Par conséquent, face à l'administration d'une preuve dactyloscopique, le rôle du juge est de rechercher non seulement si l'empreinte indiciale est probante, mais encore ce qu'elle démontre: la culpabilité, si d'autres indices convergent dans ce sens, ou l'innocence, si les empreintes de l'accusé ne correspondent pas aux traces indiciales rattachées à l'auteur ou ne concordent pas avec les autres indices analysés[633].

iv. L'univocité de l'univers déterministe

654 Chaque portion du doigt, quelle qu'elle soit, est individuelle et propre à une unique personne, ce qui exclut – pour une partie des professionnels forensiques[634] – la possibilité de déclarer un résultat possible sans être affirmatif.

[633] BENEDICT, p. 522; GALLUSER, p. 14.

[634] A ce sujet: CHAMPOD, Reconnaissance, p. 16-17.

655 Dans l'univers déterministe, les dactyloscopes ne fournissent à la Cour qu'une identification formelle[635]. Dans une telle conjoncture, soit l'identification est réalisée parce que des similitudes entre la trace et l'empreinte connue existent, soit des dissemblances trop importantes sont découvertes empêchant d'assurer l'individualisation de l'empreinte indiciale. Hormis ces deux conclusions, aucun autre résultat n'est envisageable.

656 Grâce à l'avis déterministe, les juristes sont face à une preuve univoque, sans compromis, une preuve indiscutable qui ne souffre d'aucune interprétation quant à sa nature, une preuve absolue apportant une certaine évidence sur laquelle ils peuvent se fier s'il ressort que l'analyse du scientifique a été réalisée dans les règles de l'art. L'absence d'avis qualifié implique que le juge est en droit d'estimer l'identification comme certifiée et correcte, et de penser qu'en cas de doute ou de soupçon d'erreur, l'expert dactyloscope ne conclut pas à une individualisation. C'est pourquoi, dans la pratique, la nature déterministe du processus identificatoire rassure les magistrats qui, n'ayant pas les connaissances suffisantes pour identifier une personne à l'aide d'une trace dermatoglyphe, peuvent s'appuyer complètement sur les conclusions de l'expertise.

657 Actuellement, la preuve dactyloscopique jouit ainsi d'une place privilégiée étant le seul moyen de preuve s'exprimant univoquement. Sans probabilité ou marge d'erreur citée, les magistrats sont face à une réponse du dactyloscope ne laissant pas place à la Cour d'imaginer – faussement – que deux personnes puissent produire les mêmes dessins papillaires[636].

658 N'ayant en outre pas besoin de justifier l'avis qualifié et l'univocité, l'identification formelle induit un gain de temps non négligeable pour les experts dactyloscopes et pour l'autorité judiciaire, puisqu'elle rend quasi inexistants les débats en cours de procès[637].

b. Les problématiques liées à l'exploitation et à l'administration de la preuve dactyloscopique

i. L'absence de standard minimum

659 Alors même qu'une analyse dactyloscopique ne repose pas sur un minimum de similitudes, les dactylotechniciens suisses n'ont pas le droit de fournir un avis qualifié pour éviter tout

[635] MARGOT, CHAMPOD, p. 236; MARGOT, LENNARD, Empreintes, p. 9.

[636] GYSIN, p. 12; LOCARD, T. I-II, p. 88; MARGOT, CHAMPOD, p. 236.

[637] BENEDICT, p. 521; CHAMPOD, Reconnaissance, p. 268.

risque de confusion ou d'incompréhension dans l'esprit du juge. Ces deux pratiques sont contradictoires.

660 En réfutant l'avis qualifié par manque d'univocité et en acceptant que l'expert ne prouve pas numériquement les concordances, la certitude est donnée par l'univocité, mais n'est pas démontrable mathématiquement ou objectivement.

661 Pour garantir un niveau de qualité, d'infaillibilité et d'objectivité supplémentaire de la preuve dactyloscopique, il nous semble – en accord avec le Professeur Champod[638] – obligatoire de fixer un nombre de similitudes à mettre en évidence ou tout du moins d'instaurer un intervalle et de permettre l'annonce du résultat en terme probatoire, ce qui permettrait d'assurer un minimum de certitude.

662 Certes, l'absence d'un standard numérique est en partie avantageuse augmentant les possibilités d'individualisation[639], mais ce manque de limite cause également des complications, voire des désagréments.

663 Depuis 2007, pour obtenir un résultat identificatoire indiscuté, l'expert doit être suffisamment expérimenté[640]. Consécutivement, la formation des experts doit être importante et suffisante. La surestimation de l'expérience de l'homme de l'art, voire une formation lacunaire ou critiquable, peuvent influencer les conclusions identificatoires et créer un risque quant à leur valeur, sans qu'il soit possible de contrebalancer ou confirmer à l'aide de la correspondance numérique le résultat.

664 L'expérience et les qualifications de l'expert sont donc essentielles pour déterminer la qualité des conclusions dactyloscopiques. L'établissement d'un standard numérique permettrait notamment aux dactyloscopes débutants d'effectuer avec sûreté une identification[641]. Une limite stricte ne paraît en revanche pas opportune. Un dactyloscope dont l'expérience est largement prouvée peut combler les lacunes du nombre supérieur de minuties exigé grâce à ses connaissances.

665 Il est rare qu'une demande soit effectuée par le magistrat pour connaître le degré de professionnalisme du dactyloscope auteur de l'analyse et encore moins pour savoir quelles

---

[638] BECUE, CHAMPOD, EGLI, MARGOT, p. 12 et 16; BECUE, CHAMPOD, EGLI, MORET, p. 18-10; CHAMPOD, Fingerprint, p. 7; CHAMPOD, Reconnaissance, p. 15; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; NATIONAL RESEARCH COUNCIL, p. 208 et 217 ss.

[639] Supra Partie II, Chapitre 2, I, B, 2, a, n° 618-622.

[640] Infra Partie II, Chapitre 2, I, C, 1, b, ii, n° 677 et 680-682.

[641] CHAMPOD, Reconnaissance, p. 16; MARGOT, CHAMPOD, p. 234.

capacités sont demandées pour l'examen d'une empreinte précise. Pour certifier la fiabilité et la certitude apportée par la preuve dactyloscopique, sans devoir enquêter sur les qualités du dactyloscope ou celles de l'empreinte papillaire, il nous paraît donc préférable d'établir un intervalle numérique.

666 La fixation d'un standard – qui ne saurait être trop restreint, l'exigence de six à douze minuties nous semble être un compromis idéal pour exploiter la fréquence de certains types de minuties sans baser la valeur probatoire uniquement sur l'expérience de l'expert[642] – assure la fiabilité et la certitude apportée par la preuve dactyloscopique, sans empêcher le recours au processus identificatoire qualitatif et quantitatif.

667 Certains dactyloscopes expriment de la réticence face à l'instauration d'un standard minimum en voyant dans un tel procédé l'empêchement d'analyser la qualité et la quantité des points caractéristiques et du dessin papillaire. Néanmoins, outre qu'elle n'entre pas dans la logique de l'argumentation liée à l'interdiction de l'avis qualifié, l'absence d'un standard numérique ne constitue pas le passage obligatoire pour analyser les empreintes en s'intéressant au caractère qualificatif et quantitatif.

668 L'application d'un intervalle permet de prendre en considération les particularités d'un type de minuties ou d'une direction des crêtes dermatoglyphes, et ceci en assurant une certaine fiabilité aux magistrats de fond qui peuvent s'assurer au surplus d'un nombre de minuties concordantes.

669 Ainsi, que la comparaison soit réalisée par un expert débutant ou non, le juge pourra d'une manière plus sûre se fier aux déclarations identificatoires.

670 De surcroît, l'approche holistique suisse n'est pas sans conséquence sur le plan international. Le manque d'uniformisation universelle entre cette pratique et celle empirique, ainsi que l'absence d'un standard numérique mondial est également source de difficultés.

671 Paradoxalement, alors que les scientifiques et les juristes reconnaissent que la force identificatoire provient de sa nature scientifique, sa démonstration varie d'un continent à l'autre, voire d'un pays à l'autre. Il est ainsi regrettable qu'une empreinte papillaire présentant six minuties peu fréquentes ait une valeur identificatrice formelle en Suisse, alors qu'en Grande-Bretagne, le processus d'identification se basant sur les seize minuties obligatoires, la preuve dactyloscopique ne sera pas exploitable.

[642] A ce sujet: MARGOT, CHAMPOD, p. 234.

672 Les différentes philosophies selon les pays nous amènent à nous poser la question suivante: si l'identification est certaine et fiable grâce à la science, pourquoi la preuve serait introduite en Suisse, mais niée d'office en Grande-Bretagne?

673 L'absence d'uniformisation mondiale nous permet d'affirmer que la part de subjectivité des dactyloscopes suisses n'est pas si faible qu'il n'y paraît[643]. C'est en effet par leur affirmation que la justice a reconnu qu'un standard minimum n'était pas nécessaire pour admettre une identification. Extensivement, ce sont les scientifiques eux-mêmes qui ont déclaré à la Cour à partir de quand une preuve est fiable scientifiquement, alors même que des dactyloscopes étrangers ne l'exploiteraient pas.

674 En définitive, la décision des juges suisses relative à l'identité de l'accusé est dictée presque essentiellement par les experts mettant à mal l'indépendance du magistrat. Alors qu'en théorie seul le juge est compétant pour décider sur le fond, et que l'homme de l'art ne doit jamais répondre à une question juridique même indirectement, la pratique démontre que tel n'est pas toujours le cas.

ii. L'expérience comme condition requise à l'évaluation des traces papillaires

675 Nous l'avons exposé brièvement[644], les qualifications professionnelles de l'expert dactyloscope permettent de tempérer le résultat identificatoire en l'absence de standard minimum.

676 Actuellement, il n'existe aucun programme informatique permettant de désigner quels types de minuties sont particuliers et lesquels sont fréquents. C'est pourquoi, avec l'approche holisitique, la formation des dactyloscopes s'est développée. L'étendue de l'expérience s'est imposée comme critère de fiabilité et des tests de qualité ou de vérification ont été mis en fonction.

677 La justesse d'une évaluation, notamment l'attribution d'une valeur correcte aux différents éléments de comparaison, et extensivement l'évaluation de la valeur probante scientifique, s'acquiert au fil des comparaisons avec la pratique et ne repose donc que sur la formation du dactyloscope[645].

---

643 BENEDICT, p. 521; CHAMPOD, Reconnaissance, p. 15.

644 Supra Partie II, Chapitre 2, I, C, 1, b, i, n° 663-664.

645 CHAMPOD, Fingerprint, p. 7; CHAMPOD, Reconnaissance, p. 268; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; EVETT, p. 121; NATIONAL RESEARCH COUNCIL, p. 208 et 217 ss.

678 L'appréciation de l'empreinte papillaire menant à l'identification soulève donc deux risques liés à la subjectivité de l'expert d'une part, et à son manque de formation d'autre part. La première problématique ayant déjà fait l'objet d'une exégèse[646], nous nous consacrons uniquement au problème relatif à la formation.

679 La Cour déclare la preuve dactyloscopique comme fiable car revêtant une valeur scientifique. Cette valeur étant liée aux connaissances de l'expert, si le dactylotechnicien est peu formé, les risques d'erreur identificatoire sont plus probables. Ce constat implique que les conclusions de l'expert débutant ont moins de valeur que celles de l'expert aguerri. Cependant, il serait utopique de ne recruter que des dactyloscopes expérimentés qui ne peuvent l'être qu'en acquérant des années de pratique. Les dactyloscopes débutants doivent pouvoir s'entraîner, apprendre et pratiquer.

680 Pour limiter les risques d'erreur, le service AFIS ADN certifie que les dactylotechniciens de niveau 1 – premier niveau de formation et d'expérience – n'examinent et ne se déterminent que sur des empreintes évidentes et simples, soit ayant au moins douze minuties visibles sans pour autant qu'il existe douze points caractéristiques concordants en fin d'analyse. La fiabilité des résultats dépendant de l'expérience, il n'est en revanche pas possible de conclure à la similarité de la valeur probatoire selon que l'identification à l'aide de dix minuties concordantes – par exemple – est effectuée par un expert de niveau 1 ou de niveau 3. Pourtant, aucun arrêt du Tribunal fédéral ni des tribunaux cantonaux ne référence une discussion sur la différenciation de la preuve dactyloscopique en fonction de l'expérience du dactylotechnicien. Généralement, le juge du fond se borne à affirmer que la preuve est fiable, parce qu'elle a une valeur scientifique sans prendre en compte le fait que le résultat est issu d'un processus humain.

681 Pour les juristes, l'expérience comme indicateur de valeur probante est une caractéristique abstraite. A lecture de la jurisprudence, ils n'appréhendent pas la nécessité d'examiner les connaissances et la pratique dactyloscopique de l'expert pour déterminer la force probante d'une identification papillaire.

682 Le caractère qualitatif devant être pris en considération lors de l'évaluation de la force probante, tant par l'expert que par le magistrat, le juge du fond ne doit pas simplement se borner à déclarer la preuve d'identité certaine, mais rechercher en quoi elle l'est. Quant à l'expert, son expérience influençant la valeur probatoire lorsqu'il n'existe que peu de points communs, il nous paraît essentiel qu'il motive sa décision en expliquant le poids de ses

[646] Supra Partie II, Chapitre 2, I, C, 1, b, i, n° 659 ss.

connaissances et la valeur identificatrice réelle liée à son expérience à l'aide d'un avis qualifié[647].

iii. Les risques d'erreur

683 Nous l'avons examiné[648], les tribunaux et les scientifiques sont d'avis que la dactyloscopie est un moyen probatoire fiable et que le risque d'erreur peut être nettement amoindri, jusqu'à devenir inexistant, par le fait que la trace papillaire soit analysé par deux experts expérimentés successif, que le nombre de point de concordance soit acquis, voire que les caractéristiques des minuties soient de haut niveau.

684 Or, l'affaire Mayfield démontre que, malgré ces précautions, ni les experts dactyloscopique, ni la justice n'est à l'abri d'une erreur ayant pour conséquence une "fausse identification"[649].

685 Le 11 mars 2004 vers 7h30, un attentat terroriste perpétré dans quatre trains à Madrid provoque des centaines de morts et des milliers de blessés. D'importantes investigations scientifiques sont menées par les services de police du monde entier. Le FBI collabore également à ces investigations, plus spécifiquement à l'analyse des traces digitales retrouvées.

686 Lors des investigations, la police espagnole localise un véhicule volé près de la station d'où sont partis trois des quatre trains qui ont explosés. Un système de vidéosurveillance a capturé les images de trois individus suspects qui manipulent un sac à dos avant d'entrer dans le hall de la gare. Les investigations menées sur le véhicule permettent de découvrir un sac plastique bleu rempli de détonateurs et de reliquats d'explosifs identiques à ceux utilisés pour commettre les attentats. Des traces papillaires sont retrouvées sur le sac plastique et sur la voiture.

687 Le 15 mars 2004, le FBI analyse notamment une trace digitale relevée sur ledit sac plastique. Ce service commence par comparés la trace aux millions d'empreintes présentes dans le fichier automatisé des empreintes digitales américain (AFIS).

---

[647] Infra Partie II, Chapitre 2, I, C, 2, n° 724 ss.

[648] Supra Partie II, Chapitre 2, I, C, 1, a, n° 639 ss.

[649] Information disponible sur le site internet police scientifique: http://www.police-scientifique.com/brandon-mayfield [consulté le 08.05.2016]; BECUE, CHAMPOD, EGLI, MARGOT, p. 6; CHAMPOD, Friction Ridge Skin, p. 115; EXPERT WORKING GROUP, p. 21-38; NATIONAL RESEARCH COUNCIL, p. 104-106.

688 Trois bases de données internes à AFIS sont consultées: celle des délinquants (empreintes enregistrées par les services de police), des civils (militaires ou employés du gouvernement) et celle des individus suspectés d'être des terroristes. Pour chaque base de données, le fichier propose vingt "candidats" dont une des dix empreintes de doigt correspond à la trace analysée.

689 Le 16 mars 2004, un premier expert commence par comparer la trace aux vingt premiers candidats proposés par AFIS. Dès la quatrième comparaison, le dactylotechnicien identifie un individu américain.

690 Un second expert confirme l'identification de l'individu.

691 Le nom du suspect est alors révélé, il s'agit de Brandon Mayfield. Il a été identifié grâce à sa fiche dactyloscopique de l'armée, ainsi qu'à celle établie en 1989 lorsqu'il était adolescent et avait commis un vol.

692 Le 13 avril 2004, la police scientifique espagnole interpelle le FBI dans un rapport circonstancié. Ils sont en désaccord avec le rapprochement effectué entre Brandon Mayfield et la trace papillaire. Le FBI ne prend pas acte des doutes de la police espagnole et confirme le résultat. Le service est affirmatif dès lors que des caractéristiques de niveau 3 ont été analysées et qu'il y a suffisamment de points de concordance.

693 Or, les experts espagnoles relève que sept minuties discordantes existent. Le Chef du FBI constate ce point, mais le justifie par une éventuelle superposition et par la différence de pression entre l'empreinte du suspect et la trace visualisée sur le sac plastique.

694 Le 6 mai 2004, Brandon Mayfield est arrêté et mis en détention dans un quartier de haute sécurité jusqu'au 20 mai 2004.

695 En parallèle, lors de leurs investigations, la police espagnole identifie un suspect Ouhnane Daoud. Ses empreintes se trouvent dans le fichier espagnol. La police scientifique compare donc les empreintes de Ouhnane Daoud aux traces retrouvées sur le sac plastique. Quatorze minuties concordent.

696 Le 19 mai 2004, le FBI est informé de cette identification. De nouvelles analyses sont effectuées et le 20 mai 2004, sous conditions strictes, Brandon Mayfield est libéré. Quatre jours plus tard, le FBI présente ses excuses à Brandon Mayfield et à sa famille.

697 Les causes de cette "fausse identification" sont nombreuses.

698 Le nombre inhabituel de similitudes: dix minuties identifiées comme des arrêts de ligne et des bifurcations ont été retrouvées sur l'empreinte de Brandon Mayfield. Ces similitudes sont fréquentes quant au type de minuties, mais, dans le cas particulier, elles se trouvaient au même endroit, dans le même sens et avec le même nombre de crêtes, ce qui est rare.

699 Le raisonnement des experts: le fait que dix minuties se trouvant au même endroit, dans le même sens et avec le même nombre de crêtes entre elles ont largement influencé l'avis des dactylotechniciens. Ces circonstances ont amené les experts à examiner et identifier des minuties qui étaient peu définies.

700 La prise en considération de caractéristiques de niveau 3: ces éléments sont détaillés. Cela étant, ce type de caractéristiques peut varier considérablement selon la pression effectuées ou encore le mode de révélation de la trace.

701 La mauvaise interprétation des experts pour les discordances observées: malgré que sept discordances étaient présentes, le FBI n'a pas écarté l'identification de Brandon Mayfield. Au lieu de conclure à l'exclusion du suspect, les experts américains ont déclaré que les dissimilitudes provenaient d'une superposition d'empreintes.

702 La mauvaise qualité de l'image: les dactylotechniciens du FBI n'ont jamais étudié la trace originelle. L'image reçue par les experts américains était de faible qualité.

703 Ainsi, malgré que les dactylotechniciens américains se basent sur une analyse qualitative et quantitative, ils n'existent pas de "standard minimum" du nombre de minuties concordantes obligatoires. Cela étant, même en prenant en considération un "standard minimum", les analyses effectuées par le FBI menait à une "fausse identification" au vu des erreurs grossières commises et du fait que quinze minuties concordantes avaient été trouvées.

704 L'affaire Brandon Mayfield démontre que la police scientifique n'est pas infaillible et que la culpabilité d'un suspect ne doit jamais reposer sur la seule identification dactyloscopiques.

705 Malgré que la police scientifique essaye de limiter les erreurs en mettant en place des protocoles stricts (nombre de minuties, analyse par deux experts, probabilité, etc.), les erreurs sont possibles, ce que n'envisagent pas toujours les magistrats.

706 Ainsi, force est de constater que les juristes ne devrait pas admettre la preuve identificatoire par les empreintes papillaires, mais uniquement la présomption quant à l'identité du

suspect[650]. C'est pourquoi, les dactyloscopes préconise l'emploi de la méthode ACE-V – analyse, comparaison, évaluation (probabiliste) et vérification – afin d'assurer cette présomption identificatoire et de faire état du ratio d'erreur possible, ceci permettra au dactyloscope de ne pas conclure à une identification, mais à une statistique et/ou une probabilité, méthode préconisée dans le cadre des analyses ADN[651].

iv. Le manque de formation scientifique des juristes

707 Depuis l'arrêt Daubert, pour trancher l'admissibilité de la preuve dactyloscopique, les juges américains doivent examiner si la technique ou la théorie d'intérêt a été testée, son degré d'exposition auprès de la communauté scientifique, sa marge d'erreur connue ou potentielle et son acceptation générale[652]. En Suisse, il n'existe pas de réelle procédure d'admissibilité comme celle connue aux Etats-Unis.

708 La fiabilité scientifique est confondue avec l'appréciation de la preuve. Il est généralement admis que si la preuve scientifique est certaine, alors elle revêt automatiquement une force probante non négligeable. Néanmoins, le juge du fond helvétique doit motiver sa décision d'admission, malgré l'absence de procédure précise. De l'avis des juristes, cette obligation de motivation pose un rempart suffisant pour éviter de tenir une preuve non fiable ou non pertinente pour acceptable.

709 Bien souvent, l'admissibilité d'une preuve dactyloscopique se limite à la pertinence et à la nature scientifique du moyen probatoire. Plus rarement, voire de manière extrêmement ponctuelle, le juge apprécie librement les qualifications – souvent mal appréhendées – de l'expert. Ces deux constats impliquent que, bien souvent, une preuve scientifique traditionnelle est reconnue exploitable parce qu'elle l'a toujours été et qu'elle a donc suffisamment démontré sa fiabilité[653].

710 La conséquence de cette mauvaise procédure d'admissibilité est que les juges donnent souvent leur pleine confiance à l'expert mandaté, d'autant qu'il est supposé être neutre et

---

[650] CHAMPOD, Fingerprint,, p. 7; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; NATIONAL RESEARCH COUNCIL, p. 109.

[651] BECUE, CHAMPOD, MARGOT, p. 8; BECUE, CHAMPOD, EGLI, MARGOT, p. 18-21; BECUE, CHAMPOD, EGLI, MORET, p. 9-10; CAMPELL, p. 633 et 640-641; EXPERT WORKING GROUP, p. 2-9 et 39-41; HOLDER, ROBINSON, LAUB-VANDERKOLK, Chapter 9-12 à 9-17; NATIONAL RESEARCH COUNCIL, p. 12, 90-92 et 95-98.

[652] A ce sujet: BENEDICT, p. 522-523 et 526; EXPERT WORKING GROUP, p. 22; HESLER, p. 368; HOLDER, ROBINSON, LAUB-YAMASHITA, FRENCH, Chapter 13-11 à 13-21; NATIONAL RESEARCH COUNCIL, p. 12, 90-92 et 95-98.

[653] CHAMPOD, VUILLE, p. 29; LE DOUARDIN, p. 2.

impartial. Ils omettent régulièrement de discuter en profondeur de la valeur probatoire de la dactyloscopie.

711 L'admissibilité juridique devant toutefois être tranchée par le juge, nous attendons de la Cour qu'elle soit capable de comprendre le processus et les conclusions des analyses de l'expert afin d'évaluer et de se positionner sur l'identification. Il est donc essentiel que les juristes se familiarisent avec ce mode probatoire[654].

712 Actuellement, sur les questions d'ordre technique et sur la position de l'expert dans la procédure pénale, les juristes manquent cruellement de formation.

713 Il existe peu de jurisprudence sur l'appréciation de la valeur probante de la dactyloscopie. Néanmoins, un arrêt rendu par le Tribunal pénal fédéral[655] a particulièrement retenu notre attention. Les affirmations quant à la valeur probatoire des empreintes digitales ne sont pas étayées et les juges, probablement par manque de connaissances spécifiques concernant la dactyloscopie, ont entrepris des raccourcis erronés. Dans cette affaire, l'identité du coupable a été établie au moyen de ses empreintes digitales. Corrélativement à tout processus d'identification, les empreintes ont fait l'objet d'une recherche dans le fichier AFIS, puis d'une comparaison. Le recourant affirme que la valeur probante n'est pas suffisante. Pour réfuter cet argument, le Tribunal pénal fédéral déclare : "[…], *la valeur probante d'AFIS est très élevée et reconnue scientifiquement.*".

714 Nous sommes dans l'obligation de critiquer les dires du Tribunal. Le fichier AFIS n'est qu'une banque de données fournissant une liste d'individus correspondant à l'empreinte examinée sans fournir de résultat identificatoire. La preuve identificatrice ne dépend donc pas d'une base de données, mais de la qualité de l'empreinte détectée, de la quantité des points caractéristiques, du bon déroulement du processus de comparaison réalisé par l'expert et de la vérification effectuée par le second expert. En définitive, la preuve dactyloscopique est fiable ou ne l'est pas concrètement au vu du travail du dactyloscope et de ses qualifications.

715 Ce même arrêt révèle également que le Tribunal reconnaît la preuve dactyloscopique admissible et probante uniquement parce qu'elle a une valeur scientifique reconnue. A aucun moment la décision ne mentionne un débat sur la place identificatrice des empreintes digitales dans cette affaire, sur l'interprétation de cette preuve dans le cadre juridique et encore moins sur les qualifications de l'expert ou sur le risque d'erreur pouvant exister. Cette pratique va clairement à l'encontre de l'indépendance du juge, de la libre appréciation des

[654] CHAMPOD, TARONI, RPS 1993, p. 224.

[655] RR.2007.173, c. 4.3.

preuves et de la théorie de la preuve morale demandant qu'aucune force persuasive ne soit prédéfinie[656]. Certes, le dactyloscope ne déclare pas que le suspect est coupable ou non, ceci reste une décision propre au juge. Cependant, ce dernier est lié par la portée, la fiabilité et le pouvoir identificatoire de la dactyloscopie reconnu par l'expert scientifique.

716 Pour limiter, voire éviter, la violation des principes de base relatifs à la preuve pénale, un standard fixant les principes d'interprétation scientifique, une compréhension de la terminologie dactyloscopique ainsi que la prise en considération des qualifications du dactyloscope doivent être instaurées.

717 Corrélativement à tout domaine préconisant des connaissances spécifiques, il est essentiel de former le mieux possible les juristes pour qu'ils puissent prendre connaissance correctement des conclusions, savoir ce qu'elles impliquent, entrevoir les diverses failles pouvant exister et ainsi pouvoir évaluer de façon critique le travail du dactylotechnicien. Ainsi, ils pourront poser les questions adéquates au dactyloscope, et s'intéresser de plus près à son expérience pour interpréter l'identification par les empreintes digitales dans la situation concrète sans influence, et en toute autonomie.

718 Aussi sûre qu'une science soit-elle, le travail d'analyse et de comparaison est effectué par un être humain, une erreur n'est donc pas inévitable, "*errare humanum est*". Si cette marge de risque n'est pas prise en considération, il est impossible de fournir une valeur probatoire exacte à la preuve dactyloscopique[657].

v. Les limites de l'approche déterministe

719 L'empreinte digitale, palmaire ou plantaire étant individuelle et l'analyse des points caractéristiques permettant l'identification, *a priori* l'approche déterministe est suffisante et complète. Cependant, si nous creusons, nous constatons qu'une telle approche élude les problèmes liés aux traces papillaires fragmentaires, glissées, mal déposées ou à la révélation en deux dimensions.

720 L'empreinte indiciale est une empreinte de transfert, soit l'apposition d'une forme tridimensionnelle en bidimensionnelle, impliquant nécessairement une perte d'informations quantitatives et qualitatives. De telles traces sont donc généralement appréciées sous forme de probabilités. Par exemple, lorsqu'une molécule d'ADN est exhaustivement étudiée, un avis

[656] CHAMPOD, Reconnaissance, p. 268; GALLUSER, p. 46; SCHMID, Handbuch, p. 82-83.

[657] CHAMPOD, VUILLE, p. 37.

qualifié est rendu par l'expert génétique interprétant l'individualité de la trace. En ce sens, nous comprenons difficilement pourquoi une identification papillaire ne peut pas être accompagnée d'un avis qualifié.

721 L'argument en faveur de l'approche déterministe soulignant que la Cour ne s'appuierait pas sur une preuve non-univoque est fallacieux à la vue de la reconnaissance apportée à la preuve génétique fournit en termes probabilistes. Dès lors que des différences peuvent intervenir entre une empreinte inconnue et une empreinte connue – par exemple, un arrêt de ligne net analysé directement sur le doigt est flou sur un support –, il est difficile d'admettre que la preuve dactyloscopique est noire ou blanche avec une identification réalisée ou non. Le mode de conclusion identificatoire doit être, à notre avis, remis en question.

722 L'approche déterministe ne prend pas en considération la réalité des événements, puisqu'elle ne considère pas les différences et les changements opérés entre une trace de transfert et un dessin papillaire directement exploité sur le doigt d'un individu[658]. L'identification formelle n'est par conséquent pas réaliste.

723 Nous sommes d'avis que la preuve dactyloscopique se voulant un moyen probatoire objectif, elle ne peut s'entendre que statistiquement, c'est-à-dire en excluant une certaine partie de la population et en argumentant en fonction de la force signalétique des minuties analysées.

2. Une nouvelle perspective: la nature probabiliste de l'identification

a. La démonstration relative de la réalité par l'approche déterministe

724 La critique portée à la nature déterministe, nous mène à considérer la nature probabiliste du processus d'identification papillaire.

725 Les résultats issus de l'analyse identificatoire se réalisant en aval de la commission de l'infraction et ne permettant pas d'observer directement les circonstances de l'acte délictuel, l'empreinte papillaire déposée n'est pas la fidèle représentante de la réalité et des faits.

726 Premièrement, les dessins papillaires déposés ne sont pas l'exacte image de l'empreinte du doigt.

[658] CHAMPOD, Reconnaissance, p. 16-17; MARGOT, CHAMPOD, p. 236.

727 Deuxièmement, la présence d'une empreinte ne signifie pas que l'individu auteur du dépôt est l'auteur de l'infraction, ce qui crée des imprécisions/incertitudes dans le résultat identificatoire en science forensique[659].

728 Bénéficiant d'un poids important en procédure pénale, il est essentiel que les conclusions dactyloscopiques reflètent l'état naturel des événements et de l'établissement des faits pour être les plus représentatives possible de la réalité. Cette démarche implique qu'un résultat faisant suite à une analyse d'une empreinte papillaire ne peut pas être apporté comme une identification formelle, mais une présomption.

729 Le processus d'identification n'est pas dichotomique, il s'agit plutôt de *continuum* de probabilités prenant en considération la perte d'informations liée au transfert.

b. La théorie de la nature probabiliste

730 La conceptualisation par les probabilités répond aux exigences de logique et de transparence permettant aux magistrats de mieux cerner les risques et faillibilités de la preuve dactyloscopique sans rejeter sa valeur scientifique et ce qu'elle démontre. L'appréciation probatoire est ainsi plus précise, certaine et réfléchie[660]. Le juge du fond comprenant la preuve, il peut alors l'interpréter dans son ensemble.

731 L'identification ne se présente donc plus comme une preuve d'évidence, mais comme un processus qui estime la fréquence d'apparition de ce dessin papillaire si faiblement qu'il réduit la population à un unique individu[661].

732 En outre, les probabilités mettent en perspective la force et la faiblesse de l'identification en matérialisant la fréquence signalétique des classes de minuties. Actuellement, la fréquence d'apparition de certaines configurations de minuties est déterminée par l'expert au vu de son expérience, ce qui laisse encore une part de subjectivité. Cependant, depuis une dizaine d'années, le Professeur Champod réalise des études relatives à la recherche statistique dans ce domaine.

---

[659] BIEDERMANN Alex, p. 101; CHAMPOD, Fingerprint, p. 7; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308.

[660] BECUE, CHAMPOD, EGLI, MARGOT, p. 12 et 16; BECUE, CHAMPOD, EGLI, MORET, p. 8-10; CAMPELL, p. 727-731; CHAMPOD, Fingerprint, p. 7; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; CHAMPOD, VUILLE, p. 29; LE DOUARDIN, p. 2; MARGOT, CHAMPOD, p. 237.

[661] CHAMPOD, Reconnaissance, p. 267.

733 Pour déterminer la force probante et la fiabilité de l'identification, il propose un modèle de calcul mettant en relation la probabilité que les minuties de la surface analysée soit de ce type (centre, delta, arc, boucle, verticille, etc.), la probabilité des diverses orientations relatives à ces points caractéristiques, la probabilité que les minuties combinées prennent la longueur examinée et la probabilité que ces minuties prennent l'arrangement observé. Lorsque l'expert multiplie ces différentes probabilités, il obtient un résultat déterminant "*la probabilité relative à la rareté d'une configuration de minuties dans la population*". Devant la Cour, cette probabilité permet au juge du fond d'apprécier plus objectivement la valeur probatoire – certes pas infaillible – mais réelle et objective.

734 Si, actuellement, les systèmes informatisés et l'approche déterministe[662] ont rendu obsolète la classification, une identification formelle pouvant être réalisée en quelques minutes, les discussions sur la nature probabiliste des résultats et les études du Professeur Champod risquent de renverser la tendance. Une réintégration du rôle de la classification n'est pas exclue. Grâce à elle, il serait possible d'obtenir automatiquement des données précises sur la fréquence des divers points caractéristiques, leur combinaison et ainsi fournir un résultat le plus correct possible, sans se fonder uniquement sur les données issues de l'expérience de l'expert[663].

c. L'avantage des probabilités

735 Dans le cadre juridique et probatoire, l'approche probabiliste contient de nombreux avantages. En prenant en considération la fréquence et/ou la particularité des divers types de minuties ou de leur configuration, elle contrecarre l'absence du standard numérique en Suisse.

736 Grâce à un standard prédéfini, l'expérience d'un expert ne serait alors plus déterminante et la conclusion identificatoire s'appuierait sur une plus grande objectivité tout en prenant en considération les incertitudes inévitables accompagnant l'hypothèse identificatoire. Couplé avec l'objectivation mathématique, l'expert rend une décision accompagnée d'un avis qualifié expliquant le résultat.

737 L'application de la nature probabiliste aurait pour conséquence que l'explication circonstancielle de la trace ne serait pas la seule débattue au procès. Le juge du fond appréhenderait plus aisément la force de l'identification pour l'intégrer et l'interpréter à sa

[662] Supra Partie II, Chapitre 2, I, B, 2, a, n° 613 ss.

[663] Supra Partie II, Chapitre 2, I, C, 2, a, n° 724 ss.

juste valeur dans le faisceau de preuves nécessaire à la découverte de la vérité. A noter que pour atteindre ce haut degré de discussion/débat, il est indispensable de fournir des bases probabilistes aux juristes, sans quoi ils ne pourraient pas appréhender correctement les conclusions statistiques[664].

738 En définitive, la preuve dactyloscopique serait issue d'une analyse, d'une comparaison, d'une évaluation selon des hypothèses et d'une vérification. Nous réitérons ici notre volonté de traiter la preuve dactyloscopique similairement à ce qui prévaut pour les autres traces indiciales en recentrant l'appréciation sur la liberté de la Cour et non de l'expert. Ce dernier ne fournirait dès lors qu'un argument mathématique sur l'identification, une présomption, laissant de manière certaine la décision finale aux magistrats[665].

3. L'utilisation du système AFIS et ses limites

a. Un outil efficace et précieux pour les dactyloscopes et la justice

739 Dans le domaine des empreintes papillaires, le système AFIS constitue la base de données regroupant les profils dermatoglyphes d'individus et les traces inconnues. La collection des fiches enregistrées sert ainsi à mettre en place un matériel de référence permettant l'évaluation des traces prélevées pour déterminer l'identité d'une personne.

740 Au sein de cette base, les algorithmes de recherches automatiques permettent de comparer une trace aux empreintes intégrées dans AFIS[666], et inversement, de comparer une empreinte connue par la base de données pour retrouver un potentiel lien avec une trace inconnue.

741 Le nombre d'identifications positives est intimement lié à la croissance constante des données enregistrées. Il est indiscutable que plus il existe de profils déca- ou monodactylaires, plus les chances d'obtenir un hit s'accroissent.

742 L'augmentation des profils ou des traces répertoriées offre également une base AFIS plus représentative des variabilités entre les différentes appositions des minuties.

---

[664] Sur les difficultés d'appréhender les résultats statistiques, voir: Infra Partie II, Chapitre 2, II, C, 1, b, iii, n° 1022.

[665] BECUE, CHAMPOD, EGLI, MARGOT, p. 12 et 16; BECUE, CHAMPOD, EGLI, MORET, p. 8-10; CHAMPOD, Fingerprint, p. 7; CHAMPOD, Reconnaissance, p. 267; CHAMPOD, Friction Ridge Skin, p. 115; CHAMPOD, Overview, p. 308; MARGOT, CHAMPOD, p. 238; NATIONAL RESEARCH COUNCIL, p. 109.

[666] BUQUET, p. 165; EGLI, p. 55.

743 L'intra- (même doigt) et l'intervariabilité – se définissant comme le résultat statistique au vu des différentes appositions des minuties – sont à la base de toutes approches probabilistes. Actuellement, l'approche déterministe en vigueur en Suisse ne s'appuie jamais sur le rapport de vraisemblance que peut offrir un système informatisé. Cependant, selon notre position, l'approche probabiliste est plus viable pour le juriste qui doit apprécier la preuve dactyloscopique. C'est pourquoi, il est important de souligner l'avantage de l'exploitation des scores issus du système AFIS. La collection de fiches et l'automatisation des bases de données offrent en effet la possibilité de déterminer le plus justement possible les fréquences et probabilité d'existence des points caractéristiques. Ainsi, la fréquence connue d'un type de minutie ou de la concordance avec d'autres points caractéristiques renforce la valeur identificatoire, ou au contraire, s'il n'existe que peu de minuties analysables et qu'elles sont fréquemment examinées dans cette configuration, la diminue.

744 Dans le cadre de la recherche de la vérité, il ne fait nul doute que la chance accrue d'identifier un suspect ou de blanchir un innocent, de surcroît en déterminant la fréquence d'apparition des minuties, est de grand intérêt, le but de tout procès pénal étant de punir l'auteur et de disculper l'innocent.

745 Dans tous les cas, le résultat obtenu après analyse par le système AFIS est utile au dactylotechnicien pour évaluer l'identification après comparaison entre une empreinte inconnue et une autre – connue. Le rapport de vraisemblance issu de l'utilisation des scores – indiquant la proximité entre les deux empreintes comparées – du système automatisé peut être utilisé à des fins d'évaluation de la preuve.

746 Ainsi, le renforcement des bases de données d'empreintes digitales influe sur les chances d'identification et aide les juristes à se déterminer sur la force probante d'une identification papillaire[667]. En contrepartie, avec l'évolution des systèmes informatiques – capacité de stockage grandissante, augmentation de la vitesse d'analyse, fiabilité sécuritaire, qualité des résultats, etc. –, les bases de données contiennent de plus en plus d'informations exploitables en justice, ce qui peut créer des risques d'atteintes aux droits personnels.

[667] A ce sujet: EGLI, p. 56.

b. Le traitement informatisé des empreintes papillaires à la lumière de la liberté personnelle et de la sphère privée

747 Par application de l'art. 354 CP, le service AFIS ADN enregistre et répertorie les empreintes digitales et les traces relevées par les autorités cantonales, fédérales ou les représentations de la Suisse à l'étranger. En cas d'identification positive, le service chargé de la gestion de la base de données relie le numéro de contrôle de processus avec les données personnelles contenues dans IPAS et communique les résultats avec les données à l'autorité demanderesse.

748 La recherche des concordances dans le système AFIS, voire l'intégration de la trace ou du profil décadactylaire, puis le regroupement entre le numéro de contrôle de processus et les données du fichier IPAS soulèvent un certain nombre de problèmes. Ce processus – traitement et couplement des informations – peut porter atteinte, de manière plus ou moins importante, aux droits fondamentaux de chaque personne.

749 Trois questions se posent alors: quelle est la nature de l'atteinte subie par les personnes concernées lors du traitement et du stockage de leurs données? Quels sont leurs droits? A partir de quand devons-nous déclarer qu'il est fait usage des données personnelles de manière inappropriée ou abusive?

750 La Cour européenne des droits de l'homme[668] et le Tribunal fédéral[669] sont unanimes et considèrent que la collecte, le traitement et la communication des empreintes digitales, ainsi que leur enregistrement dans un système informatisé, constituent une atteinte à la liberté personnelle (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 10 al. 2 et 13 Cst), dès lors qu'elles entrent dans la définition des données personnelles (notamment, art. 3 let. a et c LPD).

751 Contenant des informations uniques et individuelles, les empreintes digitales constituent des données à caractère personnel (art. 3 let. a LPD), considérées comme des données sensibles lorsqu'avec l'association de l'identité elles fournissent une indication sur la race (art. 3 let. c LPD)[670]. Dès lors, leur conservation et leur traitement n'est acceptable et licite qu'en

---

668 CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 84.

669 ATF 109 Ia 146, 157; SJ 1990 561, 563; ATF 113 Ia 257, 263; ATF 120 Ia 147, 149 = JdT 1996 IV 61, 61; ATF 122 I 360, 362 = JdT 1998 I 203, 204-205; ATF 128 II 259, 262 = JdT 2003 I 411; TF 1P.363/2006 du 12 septembre 2006, c. 2.2.

670 A ce sujet: DSG-BELSER, NOUREDDINE, p. 421-422 et 426; MEIER P., p. 197-198 et 201; PFPDT, Rapport 2004/2005, p. 64; ROSENTHAL, JÖHRI, art. 3 N 8 ss.

respectant les conditions de légalité, de proportionnalité et d'intérêt public prépondérant (art. 4 LPD).

752 La première et la dernière condition de l'art. 4 LPD ne créent guère de problème. Le législateur suisse a édicté des dispositions légales suffisamment précises (art. 261 CPP et les dispositions de l'Ordonnance sur les données signalétiques) indiquant aux intéressés dans quelles circonstances et sous quelles conditions l'autorité policière peut s'ingérer dans leur vie privée pour traiter des données signalétiques[671].

753 Quant à l'intérêt public, dans le cadre de la lutte contre la criminalité, il est essentiel d'identifier rapidement les potentiels criminels. Sans suspect, aucune procédure judiciaire n'a lieu d'exister, extensivement aucun crime ne peut être puni. Toute société démocratique est en droit de protéger la collectivité et de punir les criminels. La conservation des données dactyloscopiques vise ce but légitime de détection des infractions pénales et, par voie de conséquence, de prévention de celles-ci.

754 L'atteinte aux droits de la personnalité subie par l'enregistrement des données dans le système automatisé et leur regroupement en cas d'identification avec d'autres données personnelles n'est donc pas injustifiable. Faut-il encore que la proportionnalité soit respectée.

755 Dans l'affaire *S. et Marper c. Royaume-Uni*, la Cour européenne rappelle que la protection de la vie privée (art. 8 CEDH) est affaiblie de manière inacceptable si l'usage des techniques informatisées est effectué à n'importe quel prix et sans mise en balance des intérêts en présence. En particulier, la Cour estime qu'il n'est pas proportionné de conserver les données indéfiniment, ou concernant des personnes acquittées ou au bénéfice d'un non-lieu[672].

756 Ces quelques remarques d'ordre général nous amènent à nous déterminer sur le fichier AFIS, tel qu'il est conçu et exploité par le service AFIS ADN.

757 Au début du processus d'identification, la police cantonale attribue un numéro de contrôle de processus permettant la pseudonymisation des empreintes utiles à l'enquête. Le couplement de l'empreinte digitale avec l'identité de la personne, soit avec le fichier IPAS, n'est effectué que dans l'hypothèse où l'identification est réalisée. De surcroît, la transmission du résultat

---

671 CourEDH, Affaire *Leander c. Suède*, arrêt du 26 mars 1987, 9248/81, § 54-55; CourEDH, Affaire *Antunes Rocha c. Portugal*, arrêt du 31 mai 2005, 64330/01, § 67; CourEDH, Affaire *El Haki c. Belgique*, arrêt du 25 septembre 2012, 649/08, § 104.

672 CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 122.

se fait *via* une plateforme de communication spécialement créée à cet effet, ce qui permet un transfert sécurisé des données personnelles.

758 Dans ces circonstances et après investigation, le préposé fédéral à la protection des données et à la transparence a constaté que la protection des données est totalement respectée[673]. A noter que cette constatation est applicable par analogie au respect des conditions sur la protection des données imposées par les art. 95 ss CPP, lorsqu'une procédure pénale est pendante. Par conséquent, l'atteinte à la liberté personnelle et à la sphère privée est justifiée et le traitement n'est pas abusif au sens de l'art. 13 al. 2 Cst.

c. L'exception de l'art. 261 al. 2 CPP

759 A la lumière de l'évolution dans la pratique de l'identification judiciaire grâce aux empreintes digitales et de la procédure pénale unifiée, il est intéressant de constater que les risques d'atteintes illicites, voire abusives, ne sont pas inexistants.

i. Le passé, le présent et le futur possible du champ d'application personnel

760 Avant l'unification de la procédure pénale, la plupart des cantons limitaient les mesures d'identification aux seules personnes suspectées d'avoir commis un crime ou un délit. La prise d'empreintes digitales et leur éventuelle conservation ne concernaient en aucun cas les auteurs d'une simple contravention ou les tiers n'ayant pas le statut de prévenu ou de suspect.

761 Depuis l'entrée en vigueur du Code de procédure pénale fédéral, le champ d'application personnel s'est quelque peu élargi, notamment en octroyant la possibilité de saisir des données signalétiques en cas de commission d'une contravention. En outre, même s'il est exacte que – sauf application de l'exception de l'art. 261 al. 2 CPP – la conservation et l'utilisation des données signalétiques subséquentes à la procédure pénale ne concernent que les données individuelles d'une personne rendue coupable ou acquittée pour cause d'irresponsabilité, la conservation des empreintes digitales des personnes reconnues comme ne pouvant pas être l'auteur de l'infraction ou disculpées est interdite; l'insertion des

[673] Préposé fédéral à la protection des données et à la transparence, *Etablissement des faits par le PFPDT : utilisation de profils d'ADN dans les procédures pénales et à des fins d'identification de personnes inconnues ou disparues*, Berne 2005, disponible sur : http://www.edoeb.admin.ch [consulté le 08.05.2016].

empreintes digitales dans la base de données AFIS, voire la liaison avec le fichier IPAS, touche, en revanche, tout individu ayant fait l'objet d'une identification.

762 L'évolution de la pratique judiciaire dans le domaine des empreintes digitales impliquant le développement du champ d'application personnel concerne donc exclusivement la saisie et le traitement des données. Cependant, il ne faut pas perdre de vue que les pratiques changent et les mœurs aussi. L'art. 261 al. 2 CPP ouvre une nouvelle porte, celle de la conservation des données signalétiques d'une personne acquittée moyennant le respect de certaines conditions. Il est légitime de se poser la question d'un élargissement plus conséquent du champ d'application personnel. Il n'est pas inconcevable que, dans un futur plus ou moins proche, la totalité de la population soit inscrite dans ce registre informatisé.

763 Mais qu'en serait-il de la proportionnalité si une base légale était édictée dans ce sens? Vraisemblablement, une telle pratique ne devrait pas pouvoir se justifier par la nécessité de répression des infractions pénales. Elle irait à l'encontre de la présomption d'innocence et de l'interdiction du *fishing expedition*.

764 Concernant la présomption d'innocence, s'il est exact que l'inscription des empreintes digitales de la totalité de la population ne serait pas signe de soupçon, il ne fait nul doute que nous aurions tous l'impression d'être considérés comme de potentiels coupables[674].

765 Pour employer une mesure coercitive, des soupçons suffisants sur la commission d'une infraction doivent exister. La doctrine et la jurisprudence en déduisent l'interdiction d'une recherche indéterminée de moyen de preuve, nommé le *fishing expedition*[675]. Un acte de procédure ne doit pas être effectué pour obtenir une série d'informations et qui ne serait justifié qu'ultérieurement par des soupçons.

766 Actuellement, la saisie et l'enregistrement systématique des empreintes digitales de toute la population est donc incompatible avec le respect des libertés en cause. Cependant, le droit évolue. Les accords fiscaux entre la Suisse et divers Etat tiers, tel que les Etats-Unis, démontrent une volonté croissante d'échange d'informations se basant sur un ensemble de circonstances sans que de réels soupçons existent ou qu'un but déterminé ne soit visé. La

---

[674] CourEDH, Affaire *Rushiti c. Autriche*, arrêt du 21 mars 2000, 28389/95, § 31; CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 122.

[675] ATF 103 Ia 206, 211-212 = JdT 1979 IV 16; ATF 121 II 241, 242-243; ATF 122 II 367, 371 = JdT 1998 IV 127; ATF 125 II 65, 73-74; ATF 134 II 318, 327; ATF 136 IV 82, 85; MOOR, FLÜCKIGER, MARTENET, p. 989; SCHMID, Strafprozessrecht, p. 265; StPO-KELLER, art. 241 N 5.

Suisse a toujours trouvé des compromis pour éviter le *fishing expedition*[676]. Pendant, longtemps, les fiscalistes étaient inquiets de voir la limite d'un tel principe s'amoindrir de plus en plus[677]. Leurs inquiétudes se sont révélées légitimes puisque, notamment, l'échange automatique d'informations entre la Suisse et l'Union européenne sur les intérêts perçus et produits d'assurance-vie est applicable depuis le 1er janvier 2015 et s'étendera à toutes les données requises par l'OCDE dès le 1er janvier 2017. Il n'est donc pas dénué de sens de s'inquiéter qu'une recherche indéterminée d'empreintes digitales puisse se justifier – par exemple – par la croissance de la criminalité et la volonté toujours plus grande de punir les criminels au nom de la sécurité publique.

767 De la possibilité de saisir et d'enregistrer le profil en cas d'infraction de crime ou de délit, nous avons élargi ce moyen de contrainte aux contraventions et exceptionnellement aux personnes acquittées (art. 261 al. 2 CPP). Personne ne peut prédire l'avenir et exclure que la limite s'amoindrisse avec le *fishing expedition*.

768 Alec Jeffreys prône d'ailleurs le fichage génétique de l'intégralité de la population[678]. Cette volonté peut être appliquée par analogie au fichage des empreintes papillaires dès lors qu'elles visent le même but d'identifier l'auteur de l'infraction. Par ailleurs, d'après le Professeur Jeffreys, afin d'éviter des recherches de preuve sans fondement, il suffirait qu'une entité indépendante gère le fichier et que l'autorité policière puisse consulter le fichier qu'avec l'autorisation d'un juge. Les juristes doivent donc rester prudents quant à la possibilité de ficher tout un chacun.

769 Notons encore qu'aujourd'hui, le passeport biométrique nécessite la prise d'empreintes de deux doigts. Tout individu muni d'un passeport biométrique voit ses empreintes fichées. Pour l'heure, la transmission de ces données ou leur utilisation à des fins judiciaires n'est pas prévue, mais, comme énoncé précédemment, l'évolution en matière de mesure d'identification est incertaine. Il n'est dès lors pas inutile de s'inquiéter quant à la possibilité de coupler toutes ces données dans le cadre juridique, s'il est prouvé que dans le cas concret l'usage de la banque de données ISA[679] par le service AFIS ADN est nécessaire et dans l'intérêt de la sécurité publique. Ce processus correspondrait à l'idée d'Alec Jeffreys concernant le fichage génétique.

---

[676] Le Temps, *"Avec l'échange automatique, nous allons avoir quelques années difficiles devant nous"*, article du 9 avril 2015; L'Hebdo, *Les enjeux du deal avec les Etats-Unis*, article du 11 juin 2009.

[677] AMADO, MOLO, p. 545; BEHNISCH, p. 753-755; Le Temps, *4450 noms, sans amende*, article du 20 août 2009; OBERSON, p. 142.

[678] Le Monde, *Les limites des fichiers génétiques de la police*, article du 22 décembre 2003.

[679] Infra Partie II, Chapitre 3, III, B, 2, f, n° 2225.

770 La question se pose néanmoins de savoir si un intérêt public pourrait justifier le fichage des empreintes digitales de la totalité de la population et la transmission des données en cas de présomption liée à une infraction pénale. Outre se prémunir contre la criminalité, le fichage automatique de l'intégralité de la population permet d'éviter la discrimination et d'augmenter les scores effectués par la base de données et peut permettre de diminuer les erreurs judiciaires liées à un mauvais résultat identificatoire ou un résultat peu probant. Mais est-ce suffisant pour exclure l'interdiction du *fishing expedition*, ainsi que violer la présomption d'innocence?

771 En l'absence de visualisation de l'avenir, la question d'un tel traitement reste ouverte, mais il nous faut garder à l'esprit que si l'usage évolue ainsi, les atteintes à la sphère privée seront particulièrement graves.

ii. La légalité de l'exception de l'art. 261 al. 2 CPP

772 Une autre crainte liée à l'application de l'exception issue de l'art. 261 al. 2 CPP existe.

773 L'art. 261 al. 2 CPP fait exception au principe général selon lequel une personne acquittée ou ayant fait l'objet d'une ordonnance de non-entrée en matière est innocente et que, partant de là, elle a le droit de voir ses données personnelles effacées. En effet, cette disposition légale prévoit que les données signalétiques peuvent être conservées et utilisées durant dix années à compter de l'entrée en force de la décision d'acquittement ou de non-entrée en matière, si les faits permettent de supposer que les données serviront pour élucider une future infraction.

774 Dans sa jurisprudence, nous en avions fait état[680], en cas d'ingérence à l'exercice des droits garantis par la CEDH, la Cour européenne des droits de l'homme exige que la loi édictée use de termes clairs permettant à la personne concernée de connaître les circonstances et les conditions auxquelles elle est soumise lors de mesures d'identification et de conservation de ses données. Cette exigence a d'ailleurs été l'un des arguments clé du Tribunal fédéral pour déterminer si les réglementations fédérale et cantonale étaient suffisantes pour permettre le traitement de données sensibles[681]. Pourtant, la formulation de l'alinéa 2 de l'art. 261 CPP est

[680] CourEDH, Affaire *Leander c. Suède*, arrêt du 26 mars 1987, 9248/81, § 54-55; CourEDH, Affaire *Antunes Rocha c. Portugal*, arrêt du 31 mai 2005, 64330/01, § 67; CourEDH, Affaire *El Haki c. Belgique*, arrêt du 25 septembre 2012, 649/08, § 104.

[681] ATF 122 I 360, 362 = JdT 1998 I 203, 204-205.

des plus vagues. Les termes "*certains faits*", "*permettent de supposer*" et "*futures infractions*", ainsi que l'utilisation du futur – "*serviront*" – ne fournissent aucune indication concrète.

775 Quand les faits sont-ils suffisants? A partir de quelle limite devons-nous reconnaître que les données signalétiques pourraient être utiles ultérieurement? Comment déterminer si elles seront à même de permettre l'élucidation d'un acte criminel? Que signifie "*futures infractions*": est-ce une infraction ayant été commise et en cours d'investigation, ou uniquement la possibilité qu'un tel acte soit commis? Le pluriel utilisé se limite-t-il à "au moins deux infractions" ou en faut-il plus? Doivent-elles être du même genre ou d'une certaine gravité?

776 Ni le Conseil fédéral, ni la doctrine ne répondent à ces interrogations. Le message du Conseil fédéral se borne à affirmer que les risques d'abus ou l'application systématique de la clause d'exception sont évités par la subordination à l'autorisation de la direction de la procédure pour la conservation au-delà de la durée ordinaire[682]. Cet argument ne nous convainc guère!

777 Qu'il s'agisse d'une décision unique des autorités de police ou d'une décision soumise à autorisation, la différence réside dans la double analyse du respect des conditions qui n'est pas exempt du spectre de l'arbitraire. Par cette base légale, les autorités pénales ont une large marge d'appréciation pour savoir dans quel cas l'exception peut ou non être appliquée[683].

778 Quant à la doctrine, seule Sandrine Rohmer tente de reconnaître la légalité de l'exception de l'art. 261 al. 2 CPP en énonçant qu'il suffit d'utiliser cette possibilité de manière restrictive et sous couvert d'une stricte proportionnalité pour ne pas porter atteinte à la présomption d'innocence[684]. Or, même s'il nous paraît discutable de pouvoir restreindre à ce point la présomption d'innocence en restant proportionnel, la question peut rester ouverte, puisque la problématique est en amont et concerne la clarté de la base légale.

779 De même, si nous reconnaissons que l'usage abusif de cette exception est limité, voire évité, par la demande d'autorisation, la problématique de l'imprécision de la base légale demeure.

---

[682] Message, CPP, p. 1226.

[683] SCHMID, Praxiskommentar, art. 261 N 11.

[684] CR-CPP-ROHMER, art. 261 N 20-23; StPO-HANSJAKOB, art. 261 N 8.

780 Contrairement à l'obligation de précision commandée par la Cour européenne des droits de l'homme et par le Tribunal fédéral[685], il est impossible de prévoir dans quelles circonstances les empreintes digitales d'un innocent peuvent être conservées. Dès lors, un usage abusif de cet alinéa n'est pas exclu impliquant une possible atteinte au droit à l'autodétermination informationnelle (art. 13 al. 2 Cst).

781 De plus, l'art. 261 al. 2 CPP est essentiellement axé sur la prévention et ne confère pas la garantie fondamentale à toute personne d'être considérée comme innocente[686] demandant que les autorités policière et judiciaire ne tiennent pas un intéressé pour coupable alors même qu'une décision d'acquittement ou de non-lieu est entrée en force[687]. *In casu*, l'application de l'art. 261 al. 2 CPP peut laisser penser que les soupçons sur la personne subsistent durant dix ans, puisque le matériel est conservé[688].

782 Comme le relève la Cour européenne des droits de l'homme[689], ce type de disposition va à l'encontre de la présomption d'innocence (art. 6 § 2 CEDH, art. 14 § 2 Pacte II, art. 32 al. 1 Cst et art. 10 al. 1 CPP). Certes, la conservation des données personnelles n'équivaut pas en tant que telle à l'expression d'un soupçon planant sur une personne acquittée ou non-accusée, mais renforce le sentiment de cette personne de ne pas être considérée comme innocente.

783 Alors qu'en règle générale ses données personnelles doivent être effacées, il est légitime que l'individu concerné par l'exception de l'art. 261 al. 2 CPP ait l'impression d'être coupable d'un méfait. Le risque d'une telle stigmatisation est loin d'être anodin puisque la personne acquittée ou sous le couvert d'une décision de non-entrée en matière est traitée à égal avec une personne condamnée à une peine privative de moins d'une année (art. 369 al. 1 let. c CP).

784 En conséquence, à notre avis, l'application généralisée de l'art. 261 al. 2 CPP atteint à la liberté personnelle, à la sphère privée et à la présomption d'innocence de manière inacceptable. Pour qu'une telle restriction soit justifiée, la Cour européenne des droits de

---

685 ATF 122 I 360, 364 = JdT 1998 I 203, 206-207; ATF 136 I 87, 91 = JdT 2010 I 367, 370; CourEDH, Affaire *Malone c. Royaume-Uni*, arrêt du 2 août 1984, 8691/79, § 66; CourEDH, Affaire *Leander c. Suède*, arrêt du 26 mars 1987, 9248/81, § 54-55; CourEDH, Affaire *Antunes Rocha c. Portugal*, arrêt du 31 mai 2005, 64330/01, § 67; CourEDH, Affaire *El Haki c. Belgique*, arrêt du 25 septembre 2012, 649/08, § 104.

686 SCHMID, Praxiskommentar, art. 261 N 11.

687 CourEDH, Affaire *Rushiti c. Autriche*, arrêt du 21 mars 2000, 28389/95, § 31.

688 ATF 120 Ia 147, 155 = JdT 1996 IV 61, 61-62; CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 103.

689 CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 122.

l'homme affirme que l'autorité policière doit avancer de puissantes raisons, sans quoi la proportionnalité ne serait pas respectée[690]. La justification de cette conservation devrait se baser sur des critères précis, tels que la gravité de l'infraction, les arrestations antérieures, le risque élevé de récidive, la force des soupçons pesant sur la personne ou tout autre argument qui limiterait l'application de la clause d'exception[691]. En l'état, l'art. 261 al. 2 CPP nous paraît être rédigé dans des termes trop vagues pour justifier l'atteinte à la sphère privée, à la liberté personnelle et à la présomption d'innocence.

d. La durée de conservation

785 Le système automatisé des empreintes digitales est un outil précieux pour les experts dactyloscopes et pour la justice. Toutefois, son utilisation doit être contrôlée et parcimonieuse. Il est essentiel de garder à l'esprit que tout enregistrement, traitement et conservation de données personnelles ou des profils de la personnalité peut porter atteinte de manière plus ou moins importante aux garanties fondamentales de l'art. 10 et 13 Cst ainsi que de l'art. 10 al. 1 CPP – respectivement de les art. 6 et 8 CEDH et art. 14 et 17 Pacte II –, et que la condition de proportionnalité doit être particulièrement bien examinée lors de l'usage informatisé des empreintes papillaires.

786 Dans le cadre de la conservation des empreintes papillaires, l'examen de la proportionnalité quant à la sauvegarde de ces données s'effectue principalement à l'aide du facteur temps. En effet, le Tribunal fédéral a reconnu qu'il était disproportionné de conserver indéfiniment les empreintes papillaires[692].

787 Tant le Code de procédure pénale fédéral que l'Ordonnance relative au traitement des données signalétiques biométriques (AFIS-O) prévoit une durée de conservation limitée.

788 L'AFIS-O n'exige l'effacement automatique des données personnelles qu'après une durée de trente ans (art. 17 al. 3 AFIS-O). En revanche, la conservation de moindre durée est soumise à demande de l'autorité policière. Le risque qu'aucune demande ne soit réalisée n'est pas inexistant. Un oubli ou une mauvaise gestion peut influer sur l'absence des demandes laissant planer l'emploi abusif de ces données (13 al. 2 Cst).

---

[690] CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 123.

[691] CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 119.

[692] ATF 120 Ia 147, 152 = JdT 1996 IV 61, 61.

789 Avec l'évolution des bases de données et le nombre toujours croissant d'empreintes papillaires enregistrées et à défaut de demande par l'autorité compétente, la crainte de voir les données conservées durant trente années s'accroît. Pour une bonne application de l'art. 17 AFIS-O, il faudrait s'assurer d'une gestion convenable et surveillée des durées de conservations par les autorités policières cantonales.

790 En appliquant l'art. 369 CP, l'effacement des données signalétiques se fait d'office après écoulement du délai dépendant de la sanction décidée. Ainsi, le risque de la violation de la sphère privée (13 al. 1 Cst) et de l'emploi abusif des données (13 al. 2 Cst) est écarté, si tant est que le système soit correctement géré.

791 La proportionnalité semble donc respectée du point de vue de la destruction des données quelle que soit la disposition appliquée. Toutefois, ces deux dispositions ne sont pas similaires: l'une prévoit l'effacement sur demande, alors que l'autre instaure la destruction d'office après écoulement du délai. A nouveau, nous affirmons notre préférence pour l'application de l'art. 369 CP aux dépends de l'art. 17 AFIS-O, les risques de non-respect de la proportionnalité étant amoindris[693].

D. La synthèse des débats et conclusion

792 La conviction des juristes concernant la fiabilité et la valeur probatoire de la preuve dactyloscopique repose essentiellement sur des principes scientifiques qui requièrent des connaissances particulières. Alors que le juge est libre d'apprécier les preuves qui lui sont soumises, ses connaissances dans le domaine des empreintes papillaires ne lui permettent pas d'être seul décideur. Bien au contraire, aux dépends de certains principes procéduraux, telle que la libre appréciation des preuves, le juge s'en remet à la conclusion identificatoire de l'expert dactyloscope sans pouvoir ni comprendre le cheminement exacte du raisonnement, ni apprécier la valeur scientifique et juridique réelle de ce mode probatoire.

793 L'approche déterministe et l'absence d'un standard minimum renforcent la conviction du juge dans sa confiance en l'expert. Le résultat ne pouvant être que positif ou négatif, le magistrat décideur se trouve face à une preuve identificatoire d'évidence qu'il peine à discuter, puisqu'elle est univoque. Secondement, l'expérience du dactylotechnicien étant le noyau de l'analyse et de la comparaison dactyloscopique, il est naturel que le juge, se sachant

[693] Supra Partie II, Chapitre 2, I, B, 1, b, iii, n° 592 ss.

inexpérimenté dans le domaine, ne discute ni l'avis de l'expert, ni les qualifications professionnelles du scientifique.

794 Nous reconnaissons que, d'un point de vue purement scientifique, l'absence d'un standard minimum renforce les possibilités identificatoires que nous offrent les dessins papillaires. En revanche, de la vision d'un juriste, ce manque de limites est déstabilisant.

795 La loi, qu'elle soit pénale, procédurale, civile, administrative, etc., cadre les comportements des personnes physiques, morales ou des autorités étatiques en déterminant clairement jusqu'où notre comportement est légal et à partir de quand il porte à conséquence, et ce en fixant des conditions. Les juristes apprécient l'objectivité imposée par les normes légales même si parfois ils doivent apprécier ou interpréter les circonstances de fait, car ces limites imposées rassurent et évitent l'insécurité juridique.

796 Actuellement, les magistrats ne sont pas formés en dactyloscopie. Ils ne sont donc pas à même de juger des risques et des avantages de ce moyen de preuve. En sus, lorsque l'autorité policière apporte la preuve identificatoire au procès, ils ne connaissent pas la valeur des minuties, leur fréquence et le nombre de points caractéristiques en commun. Ils n'ont aucun moyen de déterminer ou de prévoir sur quelles bases objectives se forment la valeur scientifique de la preuve. Il n'est donc pas exclu qu'une empreinte ayant six minuties particulières soient identifiées par deux experts, alors que deux autres l'auraient niée; il n'est pas non plus exclu qu'une empreinte indiciale soit identifiée lors d'un procès, mais qu'une empreinte reflétant les mêmes caractéristiques ne le soit pas lors d'une autre procédure. La mise en place d'un standard minimum n'éliminera pas les risques d'erreur, ni l'incompréhension possible du juge face à la conclusion identificatoire, mais permettra de les réduire. De plus, cette limite fixe un "garde-fou" indispensable lors de comparaison par des dactyloscopes inexpérimentés et s'insère dans une politique de qualité[694].

797 L'instauration de l'approche probabiliste semble également une nécessité pour apprécier à sa juste valeur la preuve dactyloscopique. Sans avis qualifié déterminant les facilités ou les difficultés rencontrées par le dactyloscope, voire les risques d'erreur possibles, aucun débat ne peut être engagé quant à la qualité et la fiabilité de la preuve, encore moins quant à sa valeur probante. L'objectivité de la preuve dactyloscopique implique le recours aux statistiques puisque l'empreinte indiciale a subi une perte d'informations et que l'identification dactyloscopique n'est autre que l'exclusion d'une certaine population. Ces deux arguments doivent être intégrés dans le processus de décision du tribunal[695]. Grâce à

[694] CHAMPOD, Reconnaissance, p. 3.

[695] CHAMPOD, Reconnaissance, p. 265.

eux, ce moyen de preuve sera discuté, argumenté, apprécié et la valeur probatoire déterminée.

798 Pour parfaire l'appréciation de la preuve dactyloscopique, une formation adéquate des juristes tant sur la science dactyloscopique que sur les probabilités doit être proposée. L'évaluation du niveau d'individualité papillaire intègre la qualité et la quantité d'informations visibles sur l'empreinte indiciale. En outre, la perte d'informations liée au transfert entre la peau et la surface de dépôt, la technique de détection et l'expérience de l'expert jouent un rôle important dans le résultat identificatoire. La préférence pour l'une ou l'autre des méthodes de détection et de révélation de l'empreinte selon le type de surface peut influencer sur la clarté et la précision du dessin papillaire à analyser. En conséquence, le choix d'une technique de détection peu encline à fournir un bon résultat et/ou l'inexpérience du dactylotechnicien engendre une preuve dactyloscopique peu fiable et incertaine. C'est pourquoi, lors de l'appréciation de moyen identificatoire, le juge doit pouvoir discuter des risques d'erreur, des probabilités apportées au procès, des techniques scientifiques utilisées et se positionner sur la suffisance des capacités professionnelles de l'expert pour l'empreinte papillaire en question. Pour ce faire, la seule solution est d'initier les juristes à cette science et aux principes mathématiques ou techniques qui gravitent autour.

799 Actuellement, faute de pouvoir interpréter et en l'absence d'un standard minimum, la libre appréciation des preuves est partielle lors de l'exploitation d'une preuve dactyloscopique. La mise en œuvre de nos trois préconisations doit permettre de fournir une indication réelle sur la valeur probatoire de la preuve dactyloscopique, sans qu'il soit nécessaire de s'en remettre uniquement à la conclusion d'un expert. Ainsi, la décision finale appartiendra – comme le réclame la théorie – à la seule conviction de la Cour.

II. L'acide désoxyribonucléique

A. L’introduction

800 La notion allemande "*genetische Fingerabdruck*" – traduite littéralement "*empreinte digitale génétique*" – exprime clairement que l'analyse ADN est le prolongement de l'empreinte digitale, *Fingerabdruck* en allemand.

801 Outre les informations sur la santé, l'hérédité ou les caractéristiques génétiques d'une personne, une fois analysé l'ADN se transforme en profil génétique utilisable comme preuve identificatoire des auteurs d'actes délictuels.

802 Ainsi, l'ADN est un outil fascinant du point de vue scientifique, performant du point de vue policier et bénéfique pour la justice, mais n'est pas exempt de défaut[696]. L'expérience démontre que l'établissement d'un profil d'ADN et sa comparaison avec des traces biologiques fournissent des résultats rapides et accroissent la possibilité d'identifier le criminel auteur de l'infraction. C'est pourquoi, l'exploitation de cette méthode de contrainte par les services policiers et judiciaires est devenue quasi systématique.

1. Définition de l'ADN

803 L'être humain possède quarante-six chromosomes composés d'acide contenu dans le noyau des cellules. Sauf en cas d'hématie, toutes les cellules vivantes – hormis les globules rouges – comportent le même ADN et par conséquent sont génétiquement identiques[697].

804 L'ADN est une molécule filiforme composée d'une double chaîne, hélice ou brin. Chaque chaîne est formée de 3 milliards de maillons, les nucléotides constitués d'un groupement phosphate, d'un sucre et d'une base azotée. Quatre sortes de bases azotées existent: l'adénine (A), la cytosine (C), la guanine (G) et la thymine (T)[698]. En tant que molécule à deux brins, l'ADN s'illustre comme une échelle s'enroulant sur elle-même. Les échelons sont composés des nucléotides qui sont chimiquement complémentaires entre les deux chaînes: la base G est toujours face à une base C et le nucléotide A toujours face au nucléotide T[699]. L'ADN est comparable à un long texte porteur d'informations constitué de 3 milliards de lettres dont l'enchaînement des quatre bases correspond soit à un gène, soit à une région intergénétique[700]. 0,1% de l'enchainement des nucléotides varie considérablement entre les individus, ce qu'on nomme communément les polymorphismes.

805 Une infime partie de l'ADN – environ 5%[701] – est déchiffrable, il s'agit des gènes porteurs d'une information génétique renfermant la recette pour la synthèse d'une protéine (gènes de l'hémoglobine, de l'insuline, de résistance ou contenant la couleur des yeux, des cheveux,

---

[696] COQUOZ, COMTE, HALL, HICKS, TARONI, p. IX.

[697] HUYGHE, ADN, p. 23; VUILLE, Thèse, p. 34.

[698] BSK-StPO-FRICKER, MAEDER, art. 255 N 11; BUQUET, p. 179-180; KLUMPE, p. 7-8; RUCKSTUHL, DITTMANN, ARNOLD, p. 543; VUILLE, Thèse, p. 32.

[699] ALTENDORFER, p. 10; BUQUET, p. 179-180; BURR, p. 20; COMMISSION D'EXPERTS, ADN, p. 12; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 11-15; KLUMPE, p. 7-8; VIREDAZ, p. 315.

[700] ALTENDORFER, p. 11-12; BURR, p. 19-20; COQUOZ, p. 161; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 23; HUYGHE, ADN, p. 25 et 35.

[701] ALTENDORFER, p. 15; BURR, p. 21; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 23; HAUSHEER, p. 453; KLUMPE, p. 8; RUCKSTUHL, DITTMANN, ARNOLD, p. 544.

etc.). Le reste de l'ADN est composé de séquences muettes dont les connaissances actuelles ne permettent pas d'expliquer la fonction. On appelle communément cette partie de la molécule l'ADN non codant, puisque ne contenant aucune information personnelle quant à la santé de l'individu, à ses anomalies génétiques, à sa filiation, etc.[702]

806 Les analyses ADN ciblent certains des polymorphismes non-codants, appelés alors les *loci*. Avec la découverte de séquences répétitives en 1985, l'ADN fait son entrée en criminalistique[703]. Les séquences polymorphiques répétitives se caractérisent par la répétition d'une succession de bases aminées. La longueur de la séquence et le nombre de fois qu'elle se répète varient d'une personne à l'autre. L'analyse de cette variabilité – une séquence d'au moins quatre lettres (Short Tandem Repeats – STRs) se répétant de une à cinquante fois est suffisante – permet d'individualiser le matériel génétique des personnes en établissant son profil d'ADN, et représente ainsi une méthode adéquate d'identification pour la police scientifique et la justice[704]. Plusieurs séquences répétitives existent dans le génome humain, la police scientifique bénéficie ainsi d'un choix étendu d'éléments analysables et utiles à l'identification[705].

807 A noter que chacun des *loci* a deux allèles qui forment le génotype pour le *locus* considéré[706]. La combinaison des génotypes des divers *loci* d'un individu est appelé profil génétique ou profil d'ADN. Actuellement, il n'existe aucun consensus quant à la terminologie à employer pour exprimer le résultat de l'analyse des séquences polymorphiques. Deux termes sont communément utilisés "*l'empreinte génétique ou ADN*" et "*le profil génétique ou ADN*"[707]. Cependant, l'usage du mot "*empreinte*" devrait être évité. Rappelant le moyen identificatoire de la dactyloscopie, il laisse transparaître une certitude quand bien même l'analyse génétique se formule à l'aide de statistique[708]. Le terme profil est plus adéquat et devrait être privilégié. Il indique uniquement qu'une partie de l'être humain est décrit laissant percevoir plus ou moins de précision. C'est d'ailleurs cette dernière terminologie qui a été choisie par le législateur lors de la rédaction de la Loi sur les profils d'ADN.

---

[702] BSK-StPO-FRICKER, MAEDER, art. 255 ss N 11; BURR, p. 21; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 23; KLUMPE, p. 9; Message, ADN, p. 33; RUCKSTUHL, DITTMANN, ARNOLD, p. 247.

[703] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 79; JEFFREYS, p. 67-73; ROHMER, Thèse, p. 63; VUILLE, Thèse, p. 37.

[704] ALTENDORFER, p. 16; COMMISSION D'EXPERTS, ADN, p. 16; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 81; HUYGHE, ADN, p. 8; RIEDO, FIOLKA, NIGGLI, p. 301; ROHMER, Thèse, p. 63; SCHMID, Handbuch, p. 470; WERRETT, p. 21.

[705] BURR, p. 170; COQUOZ, p. 163.

[706] VUILLE, Thèse, p. 35.

[707] COMMISSION D'EXPERTS, ADN, p. 10; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 109.

[708] Infra Partie II, Chapitre 2, II, B, 2, b, n° 911 ss.

2. Où trouve-t-on de l'ADN?

808 Grâce à la présence de l'ADN dans toutes les cellules eucaryotes de notre corps, des fragments de cette molécule se déposent et s'emportent au gré des mouvements d'un individu. La présente partie se borne à déterminer les traces traditionnelles ou fréquemment analysées par la police scientifique, dès lors que juridiquement le type de traces ne joue pas un rôle fondamental dans la détermination de la valeur probatoire.

809 La catégorie des liquides biologiques regroupe le sang, le sperme, la salive et l'urine[709]:

- le sang est le liquide qui se prête le mieux aux analyses ADN grâce au nombre impressionnant de cellules se trouvant dans une infime goutte;
- le sperme offre la possibilité de trouver de l'ADN tant grâce aux spermatozoïdes qu'aux autres cellules, telles que les leucocytes ou cellules épithéliales contenues dans le liquide séminal;
- la salive est intéressante du point de vue de sa fréquence de détection sur tous les supports ayant eu un contact avec les lèvres, la langue ou tout objet ayant été porté à la bouche d'un individu;
- quant à l'urine, il s'agit d'une source subsidiaire d'ADN qui peut tout de même fournir de bons résultats.

810 La catégorie des fragments organiques contient notamment les cheveux et poils, les fragments de peau, les cellules cutanées, les pellicules ou les dents et les os[710]:

- exploités très tôt, les cheveux et les poils ont très vite déçu les criminologues dès lors que seuls ceux arrachés avec leur bulbe viable ont une réelle valeur;
- les poils d'animaux domestiques sont également une source organique. L'analyse de l'ADN de l'animal concerné permet de regrouper un individu avec la scène de crime s'il dépose des poils de son animal sur les lieux ou au contraire s'il emporte des poils de l'animal du propriétaire du lieu chez qui l'auteur s'est introduit;

---

[709] A ce sujet: ALTENDORFER, p. 31; BUQUET, PASCAL, p. 32; BURR, p. 26; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 202-203 et 210; DE VALICOURT DE SÉRANVILLIERS, p. 119; DOUTREMEPUICH, p. 967; DOUTREMEPUICH, DOUTREMEPUICH, p. 18; HAUSHEER, p. 460; HUYGHE, ADN, p. 24-25; KLUMPE, p. 14-16; RUCKSTUHL, DITTMANN, ARNOLD, p. 545.

[710] A ce sujet: ALTENDORFER, p. 31; BOBAY, RUDER, p. 28-29; BURR, p. 26; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 207-210; ; DE VALICOURT DE SÉRANVILLIERS, p. 119 ; DOUTREMEPUICH, p. 967; DOUTREMEPUICH, DOUTREMEPUICH, p. 18; HAUSHEER, p. 460; HUYGHE, ADN, p. 25; KLUMPE, p. 14-16; MENOTTI-RAYMOND, DAVID, O'BRIEN, p. 774.

- les cellules cutanées sont laissées sur tout objet entré en contact avec la peau de l'individu concerné, mais malgré la fréquence de ces traces, l'ADN s'y trouve en quantité infime et souvent dégradé. Toutefois, l'établissement d'un profil partiel, voire – dans le meilleur des cas – total n'est pas improbable;
- les pellicules ont l'avantage de se prélever de manière aisée sur tout objet ou en tout lieu entourant une personne;
- les os et les dents sont principalement analysés pour identifier un cadavre[711]. Leur résistance au temps et aux dégradations naturelles, voire aux forts dommages comme le feu, permet d'effectuer un test ADN même longtemps après le décès.

3. Les trois qualités fondamentales des traces ADN et du profil génétique

811 A l'aune des qualités fondamentales de l'empreinte papillaire, les informations génétiques nécessaires à l'établissement du profil ainsi que la molécule ADN sont pérennes, inaltérables et individuelles.

812 Il sied à nouveau de préciser que ces constats sont purement théoriques et ne doivent pas se confondre avec l'identification par l'analyse ADN qui, dès lors qu'il s'agit de mettre en relation une trace ADN avec un profil génétique contient quelques incertitudes dans l'individualisation, comme nous le verrons dans notre discussion de ce moyen de preuve[712].

a. La pérennité

813 Contrairement aux données médicales ou aux autres aspects morphologiques de l'individu – tels que les photographies –, les séquences ADN sont considérées comme stables[713]. Grâce à la division cellulaire, de notre conception à notre mort, le même enchaînement de nucléotide formant notre ADN est continuellement copié au sein des noyaux cellulaires[714].

814 Conséquemment, un accusé ayant fait l'objet d'un profilage ADN ne peut pas apporter la preuve de son innocence en alléguant devant la Cour que ses caractéristiques génétiques se sont modifiées.

---

[711] BOBAY, RUDER, p. 28-29.

[712] Infra Partie II, Chapitre 2, II, C, n° 940 ss.

[713] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 75 et 224; MALAUZAT, p. 81; ROHMER, Thèse, p. 67.

[714] OPECST, ADN, p. 10; ROHMER, Thèse, p. 50-51.

815 Ainsi, la stabilité de la molécule génétique offre un argument essentiel pour reconnaître la valeur identificatoire de l'ADN.

b. L'inaltérabilité

816 Conservé dans un lieu sec, au froid et à l'abri de la lumière, l'échantillon d'ADN ne s'altère pas avec le temps[715]. Que l'échantillon date d'un jour ou de plusieurs milliers d'années, si les trois conditions de conservation sont garanties, la force probatoire du résultat identificatoire reste inchangée[716].

817 L'humidité, la chaleur ou la lumière, principalement les rayons ultraviolets, sont trois facteurs pouvant enclencher ou accélérer le processus de dégradation[717]. Bien que les caractéristiques génétiques ne soient pas modifiées, les trois causes de dégradations peuvent rendre difficile, voire impossible, l'analyse scientifique. Une dégradation partielle du matériel génétique fournit immanquablement un résultat partiel donc moins probant, dès lors que la longueur du fragment d'ADN est interdépendante avec les chances de succès identificatoire. La conséquence de la poursuite du processus de dégradation est d'autant plus problématique. En effet, dans une telle hypothèse, les séquences ADN ne donnent plus d'indications et l'identification devient impossible.

c. L'individualité

818 L'ordre dans lequel les nucléotides déterminant l'information génétique sont placés dépend étroitement de la filiation. Dans chaque noyau cellulaire humain, l'ADN est enveloppé dans 46 chromosomes définissant notre patrimoine génétique. Lors de la fécondation d'un ovule, les vingt-trois chromosomes du spermatozoïde et les vingt-trois chromosomes de l'ovule se réunissent dans l'ovule fécondé. Ainsi, l'ordre des 3 milliards de nucléotides de notre ADN est intimement lié au patrimoine génétique de notre mère et de notre père. Cependant, par le nombre de combinaisons possibles, il reste dépendant de l'un ou de l'autre membre de la même famille.

---

[715] BSK-StPO-FRICKER, MAEDER, art. 255 ss N 13; BUQUET, p. 400; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 224.

[716] ALTENDORFER, p. 33-34; ROHMER, Thèse, p. 49.

[717] ALTENDORFER, p. 33; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 224; HUYGHE, ADN, p. 26; KLUMPE, p. 34; OPECST, ADN, p. 44. Infra Partie II, Chapitre 2, II, C, 1, b, ii, b) , n° 992-993.

819 Considérons le chromosome 1 du père et le chromosome 1 de la mère, ils sont tous deux composés d'une paire héritée en partie de leur père et en partie de leur mère. Pour le chromosome 1, il existe donc deux sortes de spermatozoïdes et deux sortes d'ovules, ce qui fournit quatre possibilités d'enfants ayant une paire chromosomique différente. Cette réflexion peut se faire sur la totalité des chromosomes. Dès lors, au moment de la fécondation, il peut exister 8 millions de spermatozoïdes différents (2x2 soit quatre sortes possibles sur vingt-trois chromosomes, ce qui nous donne 2^{23})[718]. Ce chiffre vaut de même pour le nombre d'ovules. De mêmes père et mère, il n'existe pas moins de 70'000 milliards d'ADN différents. Sachant que les nucléotides des parents proviennent de leur propre patrimoine héréditaire et que les bases peuvent s'enchaîner de diverses manières, le nombre de possibilité d'ADN différents tend vers l'infini. Il faut néanmoins relever que lors des analyses génétiques, ce n'est pas la totalité de l'ADN qui est analysée impliquant des statistiques d'individualité différentes.

820 A relever encore que certains *loci* présentent un haut taux de variation dans la population humaine tant par leur composition que par le nombre de répétitions de la séquence nucléotide. Ces *loci* sont donc très discriminatoires permettant de distinguer les individus entre eux et d'être utilisés comme moyen identificatoire[719]. A l'exception des jumeaux homozygotes, la probabilité d'avoir un profil d'ADN identique est de un sur plus d'un milliard et d'un sur cent mille en cas de lien de parenté. Il est donc quasiment improbable que deux individus aient la même attribution des gènes[720].

4. Le prélèvement du matériel biologique

821 L'identification d'un auteur d'infraction serait impossible sans confrontation entre son profil d'ADN et celui obtenu à l'aide d'une trace découverte sur les lieux de l'infraction, sur un objet ou sur la victime.

822 Les possibilités diversifiées d'obtenir un profil d'ADN et la quantité infime de matériel biologique nécessaire ont largement contribué au développement dans les sciences forensiques de l'analyse ADN[721]. L'enthousiasme porté à cette méthode s'est accompagné d'une forte reconnaissance pratique, utile et probatoire de ce moyen identificatoire.

[718] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 27-28; MALAUZAT, p. 72-73.

[719] HUYGHE, ADN, p. 31; LAVERGNE, p. 48; VIREDAZ, p. 316.

[720] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 27-28; COQUOZ, p. 167; DURUPT, p. 76; HUYGHE, ADN, p. 31; LAVERGNE, p. 48; ROHMER, Thèse, p. 48.

[721] LEZEAU, p. 38; THOMPSON, p. 22.

Néanmoins, il ne faut pas omettre que la protection par la police de la scène de crime afin d'empêcher la destruction ou la contamination du matériel génétique indiciaire, la qualité de l'échantillon, du prélèvement ainsi que le déroulement de l'analyse déterminent la force démonstrative de cette méthode scientifique[722].

a. La recherche et le prélèvement du matériel génétique

823 Dans le cadre criminel, le matériel biologique est prélevé en tant que trace indiciale, *ergo* indépendamment de la volonté de la personne concernée, ou en tant qu'échantillon provenant directement d'un individu.

i. Les traces indiciaires ou le prélèvement sur la scène de crime

824 La procédure de travail forensique se base sur la lapalissade qu'une trace n'est utilisable que si elle est trouvée.

825 La recherche de traces génétiques peut être réalisée au moyen de techniques optiques ou chimiques[723]. Dans tous les cas, le technicien se sert de matériels stériles à usage unique afin d'éviter au maximum les contaminations. Il prélève toutes les traces retrouvées sur la scène de crime, les photographies, les références, voire les mesures et les définit. Une fois le prélèvement effectué, le laboratoire conserve le matériel biologique au frais en réfrigération lente à +4° pour un court délai et en congélation à -20° pour une conservation de plus de trois jours sans quoi l'ADN se dégrade et la valeur probatoire diminue substantiellement[724].

826 Le succès du recours aux profils génétiques est intiment lié à la fréquence à laquelle chaque individu disperse du matériel biologique. Même s'il est exact d'affirmer que partout où nous passons, nous laissons des molécules d'ADN, il est incorrect de penser que tout dépôt peut servir à la comparaison en raison principalement de la mauvaise qualité du matériel biologique. En revanche, le manque de matériel ADN n'est plus une barrière. Si tant est qu'elle ne soit pas dégradée, une unique molécule est suffisante pour établir un profil d'ADN grâce à la méthode PCR[725].

---

[722] BSK-StPO-FRICKER, MAEDER, art. 255 ss N 3; VUILLE, Thèse, p. 57 et 107.

[723] A ce sujet: BUQUET, PASCAL, p. 28.

[724] A ce sujet: BUQUET, p. 180-181; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 227-230; LEZEAU, p. 39-40; OPECST, ADN, p. 44.

[725] ANCEL, p. 141; BUSCH, p. 637-638; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 44 ss; DURUPT, p. 76; ROHMER, Thèse, p. 64 et 66. Infra Partie II, Chapitre 2, II, A, 4, b, n° 832-833.

ii. Le prélèvement sur l'individu ou de type corporel

827 L'analyse de la trace indiciaire génétique trouvée sur les lieux de l'infraction permet l'établissement d'un profil d'ADN de trace inconnue. Afin de pouvoir fournir un résultat, il faut pouvoir le comparer. A noter que le matériel biologique comparé avec la trace génétique peut se décliner en diverses substances. Leur nature ne joue aucun rôle quant à la possibilité d'effectuer une analyse comparative[726].

828 En Suisse, lorsqu'il s'agit de prélever du matériel génétique, le frottis de la muqueuse jugale ou la prise de sang sont les deux techniques les plus souvent employées[727]. Dans la plupart des cas, le matériel biologique de comparaison provient d'un individu identifié: un suspect, une victime, un témoin, une personne ayant pu contaminer la scène de crime, un individu répondant aux critères d'inscription dans la base de données CODIS ou un parent proche de la personne recherchée. Dans de plus rares cas, il peut arriver qu'une trace soit comparée à une autre trace d'un profil inconnu.

829 En outre, de manière identique à ce qui prévaut pour le stockage des traces à analyser, l'échantillon prélevé sur un individu doit être conservé au sec et à l'abri de la lumière. Il doit impérativement être réfrigéré à +4°, voire congelé à -20° en attente d'une analyse de longue durée. Les consignes de conservation doivent impérativement être respectées sans quoi l'ADN se dégrade et la force probatoire de l'identification est restreinte.

b. L'analyse, la comparaison et l'identification des profils génétiques

830 L'analyse génétique est symbolisée par l'étude de la variation d'un individu à l'autre d'une répétition en tandem d'unités de bases appelées également les marqueurs, marqueurs STRs ou microsatellites. Il faut donc que le prélèvement du matériel biologique sous forme de trace indiciale ou corporelle subisse toute une série de traitements biologiques ou chimiques afin de permettre le processus identificatoire.

831 La première étape est la purification de l'échantillon, soit l'extraction et la séparation de l'ADN des globules rouges et autres impuretés[728].

---

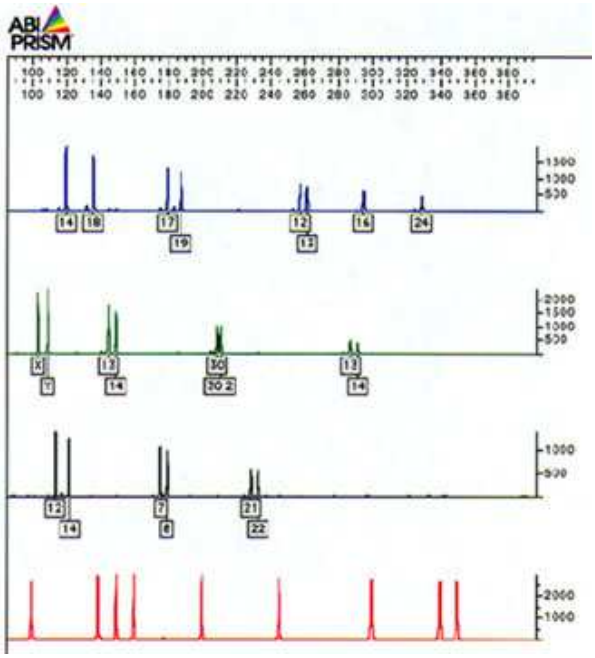
[726] ANCEL, p. 150; COMMISSION D'EXPERTS, ADN, p. 23; PITTELOUD, p. 397.

[727] BSK-StPO-FRICKER, MAEDER, art. 255 ss N 13; ROHMER, Banque de données ADN, p. 200.

[728] A ce sujet: ALTENDORFER, p. 35; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 42-43; KLUMPE, p. 16-17.

832 Après la phase d'extraction, deux possibilités existent. La quantification de l'ADN est suffisante et l'analyse proprement dite peut débuter, ou elle est insuffisante impliquant l'usage de la technique PCR. La PCR – Polymerase Chain Reaction – est une technique d'amplification de l'ADN, soit de copiage moléculaire, qui permet d'outrepasser les limites quantitatives de l'ADN[729]. Depuis l'année 2000, la technique PCR est systématiquement utilisée par les Instituts de médecine légale suisses jusqu'à une duplication de 36 fois.

833 La phase d'extraction de l'ADN ou la technique de PCR est suivie d'une électrophorèse. Aujourd'hui, les laboratoires de médecine légale utilisent le séquenceur automatique permettant d'effectuer une électrophorèse automatisée et d'obtenir un résultat informatisé. Le séquenceur automatique fourni sous forme de chiffres deux marqueurs – l'un correspond à l'allèle transmis par le père et l'autre par la mère – et ceci pour chaque séquence répétitive. A noter que plus le temps s'écoule avant d'obtenir le résultat pour un marqueur, plus l'allèle est long et donc, plus le nombre de répétitions est important avec un meilleur taux de discrimination[730].



Cette image représente le résultat d'une chromatographie. Les pics représentent les marqueurs, il peut y avoir un ou deux caractères par marqueur, soit un ou deux nombres, selon que l'allèle hérité du père et celui de la mère sont identiques (*locus* homozygote) ou différents (*locus* hétérozygote). Chaque ligne de l'électrophorégramme correspond à une couleur de fluochrome.

729 ALTENDORFER, p. 42-43; BSK-StPO-FRICKER, MAEDER, art. 255 ss N 13; BUSCH, p. 637; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 45-46; KLUMPE, p. 36-37; LAVERGNE, p. 27; RUCKSTUHL, DITTMANN, ARNOLD, p. 544.

730 COQUOZ, COMTE, HALL, HICKS, TARONI, p. 40-51.

834 Outre le gain de temps, le séquenceur automatique a l'avantage de pouvoir lire jusqu'à mille nucléotides alors que la méthode manuelle d'électrophorèse se limite à 300 nucléotides[731].

835 En fonction de l'emplacement et de la taille des microsatellites mis en évidence par le séquenceur automatique, il est possible de réaliser un profil génétique[732].

c. Le processus identificatoire et l'assistance de la base de données CODIS[733]

836 Le fonctionnement du fichier CODIS – "Combined DNA Index System" – est relativement similaire à ce qui prévaut pour le système AFIS. L'assistance de la base de données des profils d'ADN intervient à la fin du processus identificatoire. Une fois le prélèvement effectué et anonymisé, il est envoyé à un institut de médecine légale accrédité pour analyse.

837 Après l'établissement du profil d'ADN, le laboratoire l'adresse au Service de coordination ADN rattaché à l'Institut de médecine légale de Zurich[734]. Ce dernier se charge d'introduire et d'enregistrer le profil génétique au sein du fichier CODIS, le compare avec les fiches génétiques préexistantes et évalue les résultats. Lorsque les allèles de l'ADN inconnu correspondent à ceux de l'ADN d'une personne connue, la concordance est possible, sans écarter la possibilité que, sur ce *locus*, un autre individu possède les mêmes caractéristiques. C'est pourquoi il faut comparer un nombre de marqueurs suffisant et déterminer la fréquence de la composition génétique pour amoindrir les risques de concordances dues au hasard[735]. Dans le système CODIS, il était communément admis en Suisse que onze *loci* ou séquences d'ADN et le sexe étaient utilisés pour identifier une personne. Ainsi, lorsque onze marqueurs et le sexe de l'ADN inconnu et de l'ADN connu correspondaient, l'identification était réalisée[736]. Depuis 2011, le nombre de marqueurs en Suisse est passé de onze à seize. Il est important de souligner que lorsque le nombre de marqueurs nécessaires n'est pas atteint, l'identification n'est pas exclue, mais la probabilité fournie est amoindrie[737].

---

731 AMEZIANE, BOGARD, LAMORIL, p. 409-410.

732 BUQUET, p. 178; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 40-41; KAYE, p. 679; LAVERGNE, p. 28.

733 Infra Partie II, Chapitre 2, II, B, 1, b, ii, n° 886 ss; Infra Partie II, Chapitre 2, II, C, 2, n° 1030 ss.

734 BSK-StPO-FRICKER, MAEDER, art. 255 ss N 21; GIROD, MARGOT, RIBAUX, WALSH, p. 135-136; PFPDT, Rapport 2008/2009, p. 47.

735 ANCEL, p. 155; COMMISSION D'EXPERTS, ADN, p. 22; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 427; KAYE, p. 682; KLUMPE, p. 23; OPECST, ADN, p. 17; SCHWEIZER M., p. 170.

736 COMMISSION D'EXPERTS, ADN, p. 22; KLUMPE, p. 34; PITTELOUD, p. 396.

737 Infra Partie II, Chapitre 2, II, C, 1, b, ii, b), n° 994.

838 Le résultat est ensuite envoyé au Service AFIS ADN et est alors automatiquement relié avec les données relatives aux personnes ou au cas dans l'IPAS consacré à la gestion et l'indexation de dossiers et de personnes[738]. Dans l'hypothèse où une concordance appelée "hit" est décelée, le Service AFIS ADN fournit généralement le rapport de l'expert détaillé à l'autorité policière *via* une plateforme sécurisée spécialement créée à cet effet. En revanche, lorsque l'identification n'est pas possible ou que l'analyse génétique ne fournit aucun résultat, l'expert de l'Institut signifie simplement que l'identification n'est pas réalisable ou n'est pas concordante.

839 Relevons au surplus que le fichier CODIS est également capable d'analyser des correspondances lorsque deux ADN sont mélangés, par exemple parce que l'auteur a mordu sa victime et qu'au cours du prélèvement des cellules épithéliales de la victime et la salive de l'agresseur se sont jointes.

B. Les notions juridiques

840 L'autorité pénale qui soupçonne la commission d'une infraction bénéficie de divers moyens pour établir les faits et pour identifier l'auteur, notamment le prélèvement de traces matérielles telles que l'ADN.

841 A chacune des étapes du processus identificatoire à l'aide du profil génétique, il est essentiel de respecter les droits et libertés fondamentaux. En outre, la législation suisse réglemente strictement les conditions de prélèvement, d'analyse et d'utilisation des profils d'ADN.

842 Dans cette partie, nous déterminerons les conditions légales qui encadrent le processus identificatoire de l'ADN, tant du point de vue du prélèvement que de l'analyse ainsi que l'utilisation par l'autorité pénale du résultat obtenu afin de nous fournir quelques pistes de réflexion.

1. Le cadre juridique

843 Une trace matérielle ne peut être utilisée comme preuve que moyennant le respect du cadre légal fixé par les droits fondamentaux, les dispositions générales du Code de procédure pénale (art. 139 ss CPP) et les règles procédurales spécifiques au domaine en question.

[738] BUSCH, p. 641; BSK-StPO-FRICKER, MAEDER, art. 255 ss N 12.

a. Les droits fondamentaux

844 Sous l'angle international et constitutionnel, le processus d'identification est encadré par le respect des droits fondamentaux.

i. L'atteinte à l'intégrité corporelle et à la liberté personnelle causée par le prélèvement

845 La comparaison des profils d'ADN nécessite l'établissement d'au moins deux profils. L'un provient de l'analyse de la trace matérielle retrouvée. L'autre est issu du prélèvement du matériel génétique d'un individu déterminé. Dans ce second cas, le matériel génétique provient soit d'un frottis de la muqueuse jugale, soit d'une prise de sang.

846 Le prélèvement du matériel génétique de type corporel doit être effectué dans le respect de la liberté personnelle (art. 8 CEDH, art. 17 § 1 Pacte II et art. 10 al. 2 Cst). A cet égard, il est nécessaire d'examiner dans quelle mesure la sauvegarde de la sécurité publique peut justifier une intrusion au respect de l'intégrité corporelle.

847 Conformément à la jurisprudence de la Cour suprême, le frottis de la muqueuse jugale ne provoquant pas de blessure sur la peau et la prise de sang n'entraînant pas de complication, ces deux méthodes provoquent une atteinte légère à la liberté personnelle[739].

848 En cas d'assentiment de l'ayant droit, l'atteinte étant atypique, cela ne pose guère de problème. Dans l'hypothèse inverse, la protection de la liberté personnelle doit être garantie (art. 36 Cst)[740].

849 Notons au surplus que la prise de sang a été pendant longtemps privilégiée. Cependant, cette méthode créant une atteinte à l'intégrité corporelle plus importante que le frottis, elle a perdu de son prestige. Par conséquent, la tension existant entre le besoin de sécurité publique et l'atteinte à la liberté personnelle implique que – dans le respect de la proportionnalité au sens large – le prélèvement avec ponction veineuse ou piqure au doigt est subsidiaire au frottis de la muqueuse jugale[741].

---

[739] ATF 98 Ia 409, 412; ATF 112 Ia 248, 249 = JdT 1988 I 41, 42-43; ATF 124 I 80, 82 = JdT 2000 IV 24, 26; ATF 128 II 259, 269 = JdT 2003 I 411, 420 = SJ 2002 I 531, 532; ATF 134 III 241, 247 = JdT 2009 I 411, 416; ATF 136 I 87, 101 = JDT 2010 I 367.

[740] Infra Partie II, Chapitre 2, II, B, 1, a, iii, n° 854 ss.

[741] Message, ADN, p. 37; Message, CPP, p. 1196.

ii. L'atteinte à la liberté personnelle, particulièrement à l'autodétermination informationnelle, causée par l'établissement du profil d'ADN et de son intégration dans CODIS

850 Autre est la problématique liée à l'établissement d'un profil d'ADN, plus précisément à la comparaison des profils d'ADN[742].

851 Alors même que la partie d'ADN analysée n'est pas codée, que seul le sexe peut être déterminé par le profil génétique, que l'établissement et le traitement dans le système CODIS est effectué de manière anonymisée, l'établissement d'un profil d'ADN et son traitement par les autorités nationales touchent à la sphère intime des individus engendrant une problématique liée à l'autodétermination[743].

852 Le Tribunal fédéral[744] et la Cour européenne des droits de l'homme[745] ont rappelé à plusieurs reprises l'importance du respect de la sphère de protection du droit à l'autodétermination informationnelle (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 13 al. 2 Cst). Le profil génétique étant une succession de lettres permettant d'identifier avec une quasi-certitude la personne concernée, il est une donnée personnelle. Une atteinte à la liberté personnelle par le traitement du profil génétique et sa conservation existe. Conformément à la jurisprudence de la Cour suprême[746], cette atteinte doit être qualifiée de légère à partir du moment où l'analyse est effectuée sur une séquence non-codante, que les profils traités automatiquement sont anonymisés et que les profils sont conservés pour une durée limitée.

iii. L'admissibilité de la restriction aux droits fondamentaux touchés par le prélèvement et l'analyse ADN

853 La protection de la liberté personnelle et le respect de la sphère intime n'étant pas complètement supprimés, ni entièrement vidés de leur contenu lors d'un prélèvement

[742] A ce sujet, voir: Infra Partie II, Chapitre 2, II, C, 2, c, n° 1055 ss.

[743] ALTENDORFER, p. 156-157; ANCEL, p. 185; BSK-StPO-FRICKER, MAEDER, art. 255 ss N 9; BURR, p. 101; MOUSTIERS, p. 173; MÜLLER, SCHEFER, p. 164; ROHMER, Thèse, p. 65.

[744] ATF 120 Ia 147, 149 = JdT 1996 IV 61, 61; ATF 124 I 80, 81-82 = JdT 2000 IV 24, 25-26; ATF 128 II 259, 269 = JdT 2003 I 411, 420 = SJ 2002 I 531, 531-532; ATF 136 I 87, 101 = JdT 2010 I 367; ATF 138 I 331, 336-337; ATF 140 IV 57, 60.

[745] CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65; CourEDH, Affaire *Khelili c. Suisse*, arrêt du 18 octobre 2011, 16188/07, § 55-56; CourEDH, Affaire *Nikolova et Vandova c. Bulgarie*, arrêt du 17 décembre 2013, 20688/04, § 105; CourEDH, Affaire *Blaj c. Suède*, arrêt du 8 avril 2014, 36259/04, § 125.

[746] ATF 128 II 259, 269-270 = JdT 2003 I 411, 420-421 = SJ 2002 I 531, 532.

corporel, d'un traitement des données et de leur conservation, l'atteinte à l'art. 10 al. 2 Cst et/ou à l'art. 13 al. 2 Cst est juridiquement acceptable. Cette affirmation doit cependant être nuancée par le respect de l'art. 36 Cst.

854 Lorsqu'un droit fondamental est mis en péril, la restriction est soumise à trois conditions: l'atteinte doit reposer sur une base légale suffisante, être commandée par un intérêt public prépondérant et obéir au principe de proportionnalité.

855 Dans le domaine de la procédure pénale, les art. 255 ss CPP reprennent les principes édictés dans la loi sur les profils d'ADN. Cette dernière ayant été adoptée afin de fournir une base légale suffisante et uniforme relativement au traitement et à l'établissement de profils génétiques[747], il ne fait aucun doute que les articles du CPP satisfont la condition de base légale, ce d'autant que l'ordonnance sur les profils d'ADN complète la réglementation quant au prélèvement, à la conservation et au traitement des données identificatrices.

856 La légitimité de l'action étatique correspond à l'intérêt public à la sécurité de la collectivité et à la bonne administration de la justice.

857 Sur le terrain de la pesée des intérêts, l'intérêt public énoncé est confronté à la protection de la liberté personnelle (art. 10 al. 2 CP) et de la sphère intime (art. 13 al. 2 CP). Les prélèvements, l'établissement d'un profil d'ADN et l'enregistrement dans une base de données est un moyen adéquat pour confondre rapidement et avec fiabilité les auteurs d'une trace ou les récidivistes, voire de permettre des identifications internationales.

858 L'atteinte causée par les prélèvements à l'intégrité corporelle et à l'autodétermination informationnelle n'est que passagère. Pour autant qu'il ne s'agisse pas d'un échantillonnage effectué dans le cadre d'une enquête de grande envergure[748], l'accomplissement de la condition de nécessité ne pose donc aucune difficulté. De surcroît, s'il ne s'agit pas d'un moyen superflu pour la découverte de la vérité, l'atteinte légère et passagère aux droits fondamentaux pour préserver la sécurité publique paraît admissible.

859 Dans le strict respect du principe de proportionnalité, le prélèvement effectué sur une personne soupçonnée ou le traitement automatisé de ses données peut ne pas être dans un rapport raisonnable avec le but visé. C'est pourquoi le profilage ADN et sa comparaison dans

[747] Message, ADN, p. 20.

[748] ROHMER, Banque de données ADN, p. 207; ROHMER, RPS, p. 101. Infra Partie II, Chapitre 2, II, B, 1, b, n° 870.

le dessein identificatoire n'est envisageable qu'en cas de motifs avérés laissant penser que l'individu est l'auteur de l'infraction[749].

860 En conséquence, les atteintes aux droits et libertés fondamentaux de la personnalité respectent vraisemblablement les conditions de restriction de l'art. 36 Cst.

b. La réglementation nationale applicable à l'identification par l'ADN

861 La mise en œuvre et l'utilisation de l'analyse génétique sont réglementées pour la première fois en droit suisse à travers la promulgation de la loi sur l'utilisation de profils d'ADN dans les procédures pénales et l'identification des personnes inconnues ou disparues. Une partie des analyses se réalisant dans le cadre d'une procédure pénale, les normes pertinentes ont été transposées dans le Code de procédure pénale suisse[750]. La Loi sur les profils d'ADN ne s'applique plus qu'en tant que norme supplétive.

862 Le processus identificatoire basé sur l'analyse ADN est une mesure de contrainte compte tenu des risques d'atteintes légères aux dispositions constitutionnelles, sous prétexte que seul des segments non codants sont analysés[751]. A l'image de l'art. 36 Cst, l'art. 197 al. 1 let. a, c et d CPP impose le respect de certaines conditions: l'édiction d'une loi, le respect de la subsidiarité et de la proportionnalité au sens large[752]. Au surplus, cette disposition ajoute la nécessité de soupçons suffisants pour limiter l'usage d'une mesure coercitive. En outre, le relevé des données d'identification génétique pouvant être utilisé comme preuve doit respecter les règles de procédures spécifiques (art. 255 ss CPP et la Loi sur les profils d'ADN).

i. Le prélèvement d'ADN

a) Le champ d'application matériel

863 Sous couvert du principe de proportionnalité, l'établissement systématique d'un profil génétique ne peut pas être ordonné sans porter atteinte illicitement à la liberté personnelle et ressembler à du *fishing expedition*[753].

---

[749] Message, ADN, p. 35.

[750] BSK-StPO-FRICKER, MAEDER, art. 255 ss N 1; CPP-Commentario-BERNASCONI, art. 255-259 N 1; JOSITSCH, Strafprozessrechts, p. 136; MOREILLON, PAREIN-REYMOND, Intro art. 255 ss N 1; SCHMID, Handbuch, p. 470-471.

[751] ATF 128 II 259, 269 = JdT 2003 I 411, 421.

[752] Supra Partie II, Chapitre 2, II, B, 1, a, n° 563-564.

[753] Message, ADN, p. 34.

864 A la lecture de l'art. 255 CPP, le champ d'application matériel est relativement large. Les études criminologiques démontrant que, préalablement à un acte délictuel grave, l'auteur commettait bien souvent des actes plus banals, le législateur s'est refusé à établir une liste exhaustive d'infractions pouvant rendre difficile l'identification des récidivistes[754]. Il s'est borné à exclure uniquement l'usage de l'analyse pour identifier l'auteur d'une contravention (art. 255 al. 1 *a contrario* CPP), voire d'un délit dans le cadre des enquêtes de grande envergure (art. 256 CPP) dès lors qu'aucune personne partageant certaines caractéristiques n'est soupçonnée plus qu'une autre[755].

865 En apparence claire, ces deux dispositions méritent d'être délimitées de manière précise. Le terme "*élucidation*" employé dans la base légale laisse entrevoir qu'un prélèvement et un traitement ADN n'est possible que dans l'hypothèse où l'auteur n'est pas connu et qu'en outre, seule l'élucidation du crime ou d'un délit à l'origine de la mesure de contrainte est concerné. Or, cette interprétation restrictive de l'art. 255 al. 1 CPP va à l'encontre de l'esprit de la loi et ne correspond pas au but ayant déterminé la création d'une base de données[756].

866 Par conséquent, aux fins des art. 255 ss CPP, de la loi sur les profils d'ADN, de la doctrine et de la pratique du Tribunal fédéral, l'élucidation d'une activité délictueuse dont l'auteur est inconnu, l'éventualité réelle d'une commission future d'une infraction, de forts soupçons ou la facilitation de la détection des récidivistes sont autant de circonstances légales autorisant le prélèvement ADN et son traitement subséquent si un tel moyen est nécessaire[757]. De même, le Tribunal fédéral a reconnu que le prélèvement d'ADN sur une personne reconnue comme l'auteur d'une infraction doit être envisagé lorsque l'élaboration d'un profil doit permettre d'identifier l'auteur de crime ou de délits, même encore non portés à la connaissance des autorités répressives, en conformité avec l'art. 1 al. 2 de la loi sur les profils d'ADN [758], ce qui semble aller au-delà du texte claire de l'art. 255 CPP précisant que l'analyse n'est possible que pour élucider un crime ou un délit[759]. Cet arrêt a été nuancé quant à l'objectivité de la récidive dont les risques doivent être concrets et à la gravité des infractions

[754] BSK-StPO-FRICKER, MAEDER, art. 255 N 6-6b et 7-7f; StPO-HANSJAKOB, art. 255 N 9.

[755] CHARVET, n° 3-4 et 15; Message, CPP, p. 1224; MOREILLON, PAREIN-REYMOND, art. 256 N 3; StPO-HANSJAKOB, art. 256 N 3.

[756] Polizeiliche Ermittlung-VOSER, p. 380; SJ 2012 I 440, Rohmer, forumpoenale, p. 346.

[757] ATF 120 Ia 147, 152 = JdT 1996 IV 61; ATF 128 II 259, 275-276 = JdT 2003 I 411, 426-427 = SJ 2002 I 531; CPP-Commentario-BERNASCONI, art. 255 N 1; BSK-StPO-FRICKER, MAEDER, art. 255 N 6-6b; StPO-HANSJAKOB, art. 255 N 9-10; Message, ADN, p. 35-36; SCHMID, Praxiskommentar, art. 255 N 1-2 et art. 257 N 1.

[758] ATF 141 IV 87; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 219; JEANNERET, KÜHN, p. 284; MOREILLON, PAREIN-REYMOND, art. 255 N 5; MULLIS, p. 308; PERRIER DEPEURSINGE, art. 255, p. 329; ROHMER, Forumpoenal, p. 346; SJ 2012 I 440, 440.

[759] PERRIER DEPEURSINGE, art. 255, p. 329; ROHMER, Forumpoenal, p. 347.

considérées[760]. En revanche, si l'infraction considérée peut être élucidée nonobstant la preuve génétique, le recours au prélèvement ADN ne respecte alors pas la subsidiarité et, par conséquent, est disproportionné.

867 A notre avis, le fait que le prélèvement ADN soit autorisé pour des crimes et délits anciens ou futurs d'une personne appréhendée crée une insécurité juridique et un risque d'abus manifeste. En effet, la prévention d'erreurs d'identification et/ou le rôle préventif risque d'être des arguments plaidant en faveur d'un prélèvement systématique ou presque. La nuance du Tribunal fédéral déclarant qu'il faut une certaine vraisemblance n'est pas suffisante pour éviter l'abus, puisque ce terme est largement sujet à interprétation[761]. A l'instar de Sandrine Rohmer, nous pensons qu'il serait préférable de retenir comme condition restrictive la nécessité de critères de récivide avérée d'une infraction d'une certaine gravité plutôt qu'une vraisemblance, sans quoi l'atteinte serait disproportionnée. Le Tribunal fédéral a d'ailleurs, récemment, retenu que le critère concret de récidive devait être analysé[762].

b) Le champ d'application personnel

868 Concernant le champ d'application personnel, la mesure de contrainte consistant à prélever du matériel génétique peut être entreprise sur le prévenu, un tiers ou une personne décédée (art. 255 al. 1 CPP), dans le cadre des enquêtes de grande envergure (art. 256 CPP) ou en vue de l'établissement d'un profil génétique des personnes condamnées (art. 257 CPP).

869 En premier lieu, au sens de l'art. 255 CPP, la mesure de contrainte concerne:

- tout individu prévenu d'une infraction à la suite d'une dénonciation, d'une plainte ou d'un acte de procédure accompli par l'autorité pénale (art. 255 al. 1 let. a CPP). Il doit donc s'agir d'une personne physique (art. 111 CPP) – ce qui exclut les représentants d'une entreprise partie à la procédure (art. 112 CPP) ou les personnes appelées à donner des renseignements (art. 178 let. d à f CPP)[763] – sur laquelle pèsent des soupçons raisonnables laissant penser qu'elle est l'auteur d'un crime ou d'un délit, même anciens ou futurs qui n'ont pas encore été portés à la connaissance des autorités répressives[764];

[760] TF 1B_111/2015 du 20 août 2015, c. 3.1.

[761] ROHMER, Forumpoenal, p. 348.

[762] TF 1B_111/2015 du 20 août 2015, c. 3.1.

[763] BSK-StPO-FRICKER, MAEDER, art. 255 N 11; CPP-Commentario-BERNASCONI, art. 255 N 6; SCHMID, Praxiskommentar, art. 255 N 8; StPO-HANSJAKOB, art. 255 N 12.

[764] Message, ADN, p. 35; ROHMER, Forumpoenal, p. 346; SJ 2012 I 440, 440.

- un tiers (art. 255 al. 1 let. b CPP faisant exception au principe général de l'art. 251 al. 4 CPP) dans le strict respect de la nécessité, si le prélèvement s'avère utile pour différencier les traces indiciales suspectes de celles laissées par la victime (art. 116 CPP) ou les personnes habilitées à se trouver sur les lieux de l'infraction[765]:
- ou une personne décédée. Dans l'hypothèse où le prélèvement est utile pour clarifier l'identité du défunt ou pour confirmer/infirmer la participation du défunt à un acte délictuel[766]. En revanche, l'identification d'un cadavre inconnu ou l'élucidation d'un décès extraordinaire n'entre pas dans le champ d'application de l'art. 255 al. 1 let. b CPP qui limite l'analyse au cadavre de la victime, mais de l'art. 255 al. 1 let. d CPP concernant le matériel biologique indiciaire pouvant servir comme moyen de preuve.

870 En second lieu, l'analyse ADN lors d'enquêtes de grande envergure a pour but de confondre l'auteur ou d'exclure la participation d'une personne grâce à l'élaboration de profils d'ADN de diverses personnes physiques qui présentent certaines caractéristiques similaires à l'auteur présumé – couleur de peau et langue, par exemple – ou qui sont en lien avec la commission de l'infraction. Aucun soupçon, au sens de l'art. 197 al. 1 let. b CPP, n'étant formellement émis contre une personne, mais se rapportant à un acte délictuel déterminé, la prudence est de rigueur dans la mise en œuvre de cette disposition pour limiter les risques d'atteintes à la présomption d'innocence ou d'investigation au faciès. Afin d'éviter les dérives, le prélèvement ne peut se concevoir que si des traces indiciaires suffisantes ont été relevées sur la scène d'un crime, qu'il est ordonné par le tribunal des mesures de contrainte – contrairement aux mesures de surveillance secrète, une simple autorisation (art. 272 CPP) n'est pas suffisante – et dans le strict respect du principe de proportionnalité, notamment en visant uniquement des personnes caractérisées[767].

871 En dernier lieu, le prélèvement et l'établissement d'un profil d'ADN peut concerner des personnes condamnées (art. 257 CPP). Les termes "*personnes qui ont été condamnées*" s'entendent largement, soit comme toute personne envers laquelle une sanction pénale a été ordonnée en vertu d'une décision ayant force de loi (art. 437 CPP) et contenant l'énoncé du

[765] BSK-StPO-FRICKER, MAEDER, art. 255 N 12; JEANNERET, KÜHN, p. 283; Polizeiliche Ermittlung-VOSER, p. 383; SCHMID, Handbuch, p. 472.

[766] Message, CPP, p. 1223.

[767] BSK-StPO-FRICKER, MAEDER, art. 256 N 3 ss; CHARVET, n° 17 et 19; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 242; RIKLIN, Strafprozessordnung, art. 256 N 1; ROHMER, RPS, p. 101; RUCKSTUHL, DITTMANN, ARNOLD, p. 253; StPO-HANSJAKOB, art. 256 N 6.

prélèvement de l'échantillon ADN (art. 81 al. 4 let. e CPP)[768]. Ce type de prélèvement concerne:

- les personnes condamnées pour la commission intentionnelle d'un crime à une peine privative de liberté de plus d'une année;
- les personnes condamnées pour la commission intentionnelle d'un crime ou d'un délit contre la vie, l'intégrité physique ou l'intégrité sexuelle;
- les personnes contre qui une mesure thérapeutique ou d'internement a été prononcée. Dans cette hypothèse, la notion de "*personne condamnée*" doit être comprise largement, puisqu'elle englobe les personnes acquittées pour cause d'irresponsabilité pénale qui sont internées ou font l'objet d'une mesure thérapeutique.

872 L'intégration des profils des personnes acquittées pour cause d'irresponsabilité faisant l'objet d'une mesure thérapeutique ou d'un internement, ainsi que des coupables est justifiée par la prévention des actes délictuels, soit la détection des récidivistes[769]. L'art. 257 ne doit cependant pas être compris comme une limitation de l'art. 255 CPP, dès lors que les conditions restrictives de prélèvement ne concernent que des personnes déjà condamnées. Dans la pratique, l'art. 257 CPP a perdu de son importance et est appelé à devenir désuet dans la mesure où le prélèvement est généralement effectué durant la procédure d'investigation (art. 255 CPP)[770].

873 A noter que l'art. 257 CPP a été instauré pour élaborer une base de données des délinquants particulièrement dangereux afin de faciliter la détection des récidives. En accord avec Thomas Hansjakob, Sandrine Rohmer et Niklaus Schmid, il nous semble vraisemblable que l'art. 257 let. c CPP concernant les personnes internées ou faisant l'objet de mesure thérapeutique ne devrait être mis en œuvre que dans l'hypothèse où un crime ou un délit contre la vie, l'intégrité physique ou l'intégrité sexuelle a été perpétré, ou si une peine de plus d'une année de privation de liberté aurait pu être prononcée, tel que cela prévaut pour les let. a et b[771]. En effet, le recours systématique à l'enregistrement du profil d'ADN de ce type d'individu viderait le but visé par l'art. 257 CPP. Le libellé de la disposition étant imprécis, le

---

[768] CPP-Commentario-BERNASCONI, art. 257 N 4; Message, CPP, p. 1224; RUCKSTUHL, DITTMANN, ARNOLD, p. 251; SCHMID, Praxiskommentar, art. 257 N 3; StPO-HANSJAKOB, art. 257 N 2-4.

[769] ATF 128 II 259,270-271 = JdT 2003 I 411; TF 2C_257/2011 du 25 octobre 2011, c. 6.7.4; Message, ADN, p. 36.

[770] BSK-StPO-FRICKER, MAEDER, art. 257 N 2-3; CR-CPP-ROHMER, art. 257 N 7; Message, ADN, p. 36; Polizeiliche Ermittlung-VOSER, p. 385; SCHMID, Handbuch, p. 487; SCHMID, Praxiskommentar, art. 257 N 2; StPO-HANSJAKOB, art. 257 N 1.

[771] CR-CPP-ROHMER, art. 257 N 14; SCHMID, Praxiskommentar, art. 257 N 7; StPO-HANSJAKOB, art. 257 N 4.

Tribunal fédéral tranchera probablement à partir de quand il est possible de prélever le matériel génétique des personnes condamnées.

c) La compétence

874 L'autorité compétente pour ordonner l'analyse ADN est déterminée en fonction de la phase procédurale durant laquelle le prélèvement est effectué et dépendamment du moyen utilisé.

875 La compétence d'ordonner le prélèvement invasif – effectué à l'aide d'une prise de sang ou de cheveux non-détachés du corps – appartient au ministère public ou aux tribunaux (art. 198 al. 1 let. a CPP) au vu de l'intensité de l'atteinte à la liberté personnelle[772]. En revanche, il doit toujours être exécuté par un médecin ou un auxiliaire médical (art. 258 CPP).

876 Le frottis de muqueuse jugale causant une atteinte faible aux droits fondamentaux, le recours à l'approbation d'une instance juridique n'est pas nécessaire[773]. Pour alléger la procédure et éviter des complications inutiles, notamment la convocation des personnes concernées par la mesure coercitive, les prélèvements corporels non-invasifs peuvent être ordonnés par la police (art. 255 al. 2 let. a CPP en application de l'art. 198 al. 1 let. c CPP). Le terme "*ordonner*" doit s'interpréter largement: la police non seulement autorise le prélèvement, mais elle l'effectue[774]. En outre, dès lors que "*qui peut le plus peut le moins*", le ministère public, les tribunaux et la direction de la procédure du tribunal en cas d'urgence sont également compétents (art. 198 al. 1 let. b CPP). A noter qu'en revanche, l'analyse de l'échantillon même prélevé par la police ne peut être ordonnée que par le ministère public ou le tribunal[775].

877 Dans la mesure où il est ordonné hors perquisitions (art. 241 à 254 CPP), fouilles ou examens, et conformément à la mission de la police (art. 306 al. 2 let. a CPP), cette dernière est compétente pour ordonner l'établissement du profil génétique à partir de matériel

---

[772] CR-CPP-ROHMER, art. 255 N 25; EICKER, HUBER, p. 174; Message, CPP, p. 1223; RIEDO, FIOLKA, NIGGLI, p. 306; SCHMID, Praxiskommentar, art. 255 N 12.

[773] ATF 128 II 259, 269 = JdT 2003 I 411, 420 = SJ 2002 I 531, 532; ATF 134 III 241, 247 = JdT 2009 I 411, 416; TF 1B_685/2011 du 23 février 2012, c. 3.2; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 241; Message, CPP, p. 1223; PERRIER DEPEURSINGE, art. 255, p. 329; Polizeiliche Ermittlung-VOSER, p. 385; SCHMID, Handbuch, p. 474; SCHMID, Praxiskommentar, art. 255 N 12.

[774] CPP-Commentario-BERNASCONI, art. 255 N 15; MOREILLON, PAREIN-REYMOND, art. 255 N 10; MULLIS, p. 311; PITTELOUD, p. 399; RIKLIN, Strafprozessordnung, art. 255 N 6.

[775] ATF 141 IV 87, 90-92 = JdT 2014 IV 280, 282-283; MOREILLON, PAREIN-REYMOND, art. 255 N 10; MULLIS, p. 311.

indiciaire directement transmissible au laboratoire (art. 255 al. 2 let. b CPP)[776]. Dans les autres cas, le ministère public, les tribunaux et la direction de la procédure (art. 198 al. 1 CPP) ont la compétence d'ordonner le prélèvement. Cette exception au principe général de l'art. 182 CPP se justifie par la nature non-coercitive des traces biologiques puisqu'elles servent principalement à alimenter la base de données ADN sans être liée à un accusé[777].

878 Relevons que la police est compétente également pour ordonner le prélèvement et l'analyse subséquente d'un échantillon prélevé sur une personne décédée sans qu'il y ait mort suspecte. En revanche, s'il est utile de clarifier le déroulement de faits mortels, l'identité du défunt (art. 253 al. 1 CPP) ou de découvrir un lien entre lui et un acte criminel, la compétence revient au ministère public (307 al. 1 et 309 al. 1 let. b CPP)[778].

879 Au surplus, l'analyse d'échantillons prélevés lors d'enquêtes de grande envergure ou sur des condamnés est soumise à un régime particulier.

880 Dans le premier des cas, le prélèvement et l'analyse sont ordonnés par le tribunal des mesures de contrainte sur requête du ministère public (art. 256 CPP). La restriction à l'intégrité corporelle et au droit à l'autodétermination informationnelle touchant des personnes qui n'ont pas occasionné l'exécution de la mesure par leurs actes, mais uniquement par leurs caractéristiques spécifiques, ce régime particulier se justifie pour préserver au mieux la présomption d'innocence et le principe de proportionnalité[779].

881 Concernant les personnes condamnées, le tribunal ayant rendu le jugement est habilité à prononcer la mesure de contrainte (art. 257 CPP). Le tribunal de première instance ou la juridiction d'appel prononçant les condamnations, les internements ou les mesures thérapeutiques sont donc compétents, contrairement au tribunal des mesures de contrainte ne prononçant aucune peine ou mesure et, même si cela paraît contraire à l'art. 255 CPP, le ministère public. Ordonnée par jugement, l'analyse d'ADN ne peut être effectuée qu'une fois ce jugement devenu exécutoire[780].

[776] CR-CPP-ROHMER, art. 255 N 30; SCHMID, Praxiskommentar, art. 255 N 14.

[777] Message, CPP, p. 1223; SCHMID, Praxiskommentar, art. 255 N 15.

[778] CR-CPP-ROHMER, art. 257 N 29; Message, CPP, p. 1223; SCHMID, Praxiskommentar, art. 255 N 10.

[779] CHARVET, n° 32; Polizeiliche Ermittlung-VOSER, p. 389; SCHMID, Praxiskommentar, art. 256 N 1-2.

[780] Message, CPP, p. 36; Polizeiliche Ermittlung-VOSER, p. 384-386; SCHMID, Praxiskommentar, art. 257 N 3.

d) L'exécution de la mesure

882 Le choix du mode de prélèvement dépend de la possibilité et de la suffisance d'effectuer un échantillonnage par frottis. Néanmoins, qu'il s'agisse d'employer l'une ou l'autre des mesures, la question de l'assentiment se pose (art. 119 al. 2 let. f Cst). Les mesures d'enquête et d'instruction poursuivant un but de sécurité publique, des exceptions sont instituées lorsque l'approbation n'est pas donnée.

883 Contrairement à ce qui prévaut pour les données signalétiques (art. 260 al. 4 CPP), le recours à la force ne fait pas l'objet d'un article particulier pour l'analyse ADN impliquant l'application du principe général (art. 200 CPP).

884 Sous couvert du respect du principe de proportionnalité au sens large et à défaut d'assentiment, le ministère public ou le tribunal est habilité à ordonner l'exécution de la mesure.

885 En pratique, le recours à la force pour le prélèvement d'ADN est admis qu'après opposition de la personne au prélèvement non-invasif. Dans le cas où la personne s'oppose au frottis de la muqueuse jugale, la police n'est pas en droit de la contraindre par la force à ouvrir la bouche et n'est pas habilitée à ordonner une prise de sang. Lorsque l'opposition d'obtempérer est manifeste, seul le recours à un moyen invasif ordonné par le ministère public ou les tribunaux reste possible[781].

ii. L'établissement d'un profil d'ADN et son intégration dans CODIS

886 L'établissement du profil d'ADN doit être ordonné, selon les cas, par le ministère public, les tribunaux ou la direction de la procédure du tribunal en cas d'urgence, voire dans une unique circonstance, celle des traces indiciales – par la police (art. 255 CPP, art. 259 CPP *cum* art. 8 al. 1 Loi sur les profils d'ADN et art. 2 Ordonnance sur les profils d'ADN)[782]. Une fois ordonné, l'un des six laboratoires accrédités par le Département fédéral de justice et police réceptionne l'échantillon anonymisé par un numéro d'identification (art. 259 CPP *cum* art. 8 al. 2-3 Loi sur les profils d'ADN) afin de l'analyser.

887 L'autorité chargée de l'enquête ne communique jamais l'identité du donneur, mais uniquement le numéro d'identification. Dans certaines circonstances, le matériel biologique à

[781] BUQUET, p. 185; CR-CPP-ROHMER, art. 259 N 7-8; Message, ADN, p. 37.

[782] Supra Partie II, Chapitre 2, II, B, 1, b, i, c), n° 874 ss.

traiter peut être accompagné de données complémentaires impératives pour le travail des experts et l'évaluation de la valeur probante scientifique tout en respectant la protection des données. Le laboratoire est notamment en droit de connaître le lieu où le prélèvement de la trace a été effectué, le temps qu'il faisait, le nombre de personnes potentiellement impliquées, la race de la ou des personnes suspectées – certaines caractéristiques ayant une fréquence différente selon l'origine ethnique influant sur les données probabilistes –, ou encore, s'il existe un lien de parenté entre les suspects[783].

888 En parallèle à la transmission de l'échantillon au laboratoire, l'autorité d'enquête transmet au service AFIS ADN le numéro d'identification et l'identité du donneur pour intégrer provisoirement ces informations dans le fichier IPAS distinct de la base de données CODIS. Cependant, les profils des victimes, des personnes habilitées à se rendre sur les lieux de l'infraction, des personnes ne pouvant être l'auteur dans le cadre des enquêtes de grande envergure, lors d'un crime ou d'un délit ou en cas de non-lieu ne doivent jamais être saisies dans le CODIS (art. 11 al. 4 Loi sur les profils d'ADN).

889 Une fois le profil d'ADN établi, un résultat peut être fourni (art. 2 al. 1 Loi sur les profils d'ADN). Le laboratoire qui a effectué l'analyse transmet les résultats au service de coordination ADN qui soumet le nouveau profil à la base de données CODIS (art. 3 et 10 al. 2 Ordonnance sur les profils d'ADN).

890 La base de données des profils d'ADN gérée par le service ADN AFIS de la Fedpol (art. 8 Ordonnance sur les profils d'ADN) contient une collection organisée d'informations liées à des traces prélevées ou à des individus fichés. Ainsi, les autorités peuvent effectuer rapidement trois types de comparaison: entre des traces biologiques fichées et une trace retrouvée sur les lieux d'une infraction permettant de lier diverses affaires entre elles; entre une trace biologique inconnue découverte sur la scène de crime et le profil génétique d'un individu fiché permettant de vérifier si une personne fichée est l'auteur de la trace découverte; entre le profil d'ADN d'une personne connue et les traces biologiques fichées pour déterminer si l'individu suspecté n'est pas impliqué dans une autre procédure.

891 En cas de hit, le service AFIS ADN relie les profils génétiques aux données contenues dans IPAS, puis fournit le résultat à l'autorité requérante – autorité policière ou d'enquête – contenant le numéro de contrôle, le nom, le prénom et la date de naissance de la personne concernée (art. 10 al. 3 à 6 Ordonnance sur les profils d'ADN).

[783] Message, ADN, p. 39.

892 Sans cause ou demande de radiation subséquente et en cas de concordance, les profils enregistrés provisoirement dans CODIS sont conservés en respectant les délais légaux[784]. Dans l'hypothèse inverse, les profils d'ADN sont effacés.

iii. La conservation des données génétiques

a) La destruction des échantillons

893 L'échantillonnage prélevé est composé de l'ADN dans son intégralité, soit la partie non-codante et la partie codante. Cette dernière fournissant des indications sur l'état de santé et les caractéristiques personnelles d'un individu, un échantillon d'ADN est considéré comme une donnée personnelle, plus exactement une donnée sensible (art. 3 let. a et c LPD). C'est pourquoi la conservation des échantillons ne peut pas être illimitée dans le temps sans violer le principe de proportionnalité et cause une atteinte aux libertés personnelles[785].

894 Le Code de procédure pénale suisse ne prévoit aucun délai de conservation, contrairement à ce qui prévaut pour la conservation du dossier de procédure (art. 103 CPP), la conservation des données signalétiques (art. 261 CPP) et la réglementation générale sur le traitement des données (art. 95 ss CPP). Cependant, par renvoi de l'art. 259 CPP, la loi sur les profils d'ADN prévoit la destruction des échantillons sur demande de l'autorité qui a ordonné la mesure lorsqu'ils ne sont plus nécessaires à la procédure – si le profil d'ADN a déjà été établi (art. 9 let. a Loi sur les profils d'ADN); après trois mois, si l'autorité n'a pas prescrit d'analyse (art. 9 let. b Loi sur les profils d'ADN); ou si la personne en cause ne peut pas être l'auteur du crime ou du délit (art. 9 let. c Loi sur les profils d'ADN).

895 En outre, dès que le profil d'ADN remplit les exigences de qualité nécessaires à un traitement automatisé (art. 10 à 13 Loi sur les profils d'ADN), mais au plus tard trois mois après l'avoir réceptionné, le laboratoire est chargé de détruire l'échantillon (art. 9 al. 2 Loi sur les profils d'ADN).

896 Il ne fait aucun doute que la conservation des échantillons d'ADN serait apte à permettre de nouvelles analyses en cas de contestation ou lors de l'apparition d'une nouvelle technique d'examen[786]. Cependant, ce n'est pas la seule alternative. La possibilité d'effectuer un

[784] Infra Partie II, Chapitre 2, II, B, 1, b, v, b), iii, n° 893 ss.

[785] ATF 124 I 80, 81-82 = JdT 2000 IV 24, 25-26; ATF 128 II 259, 268-270 = JdT 2003 I 411, 419-421 = SJ 2002 I 531, 532; TF 1C_51/2009 du 26 février 2009, c. 3.1.

[786] FIAUX, p. 3; ROUX, p. 188.

nouveau prélèvement abonde dans le sens d'une prédominance de l'intérêt de la personne concernée à voir ces données sensibles effacées comparativement à l'intérêt public de lutte contre la criminalité. Le respect du principe de nécessité et de proportionnalité justifie la destruction immédiate ou le délai relativement bref de trois mois instauré par la loi.

b) L'effacement des profils d'ADN

897 L'effacement des profils est réglementé par un régime distinct de celui des échantillons puisque l'échantillonnage et les profils ne sont pas similaires tant dans la nature que dans la quantité d'informations qu'ils contiennent. En effet, la Cour européenne des droits de l'homme a relevé qu'un profil d'ADN contenait moins d'informations relevant de la vie privée, notamment des données sensibles, qu'un échantillon[787]. C'est pourquoi un délai de conservation plus long est acceptable du point de vue du respect du principe de la proportionnalité.

898 Concernant les profils d'ADN des personnes, l'art. 16 Loi sur les profils d'ADN prévoit notamment une destruction: sitôt qu'il s'avère, au cours de la procédure, que la personne en cause ne peut être l'auteur du crime ou du délit (let. a); lorsque la personne en cause est décédée (let. b); lorsque la procédure en cause est close par un acquittement entré en force (let. c); un an après le non-lieu (let. d); cinq ans après l'expiration du délai d'épreuve en cas de sursis à l'exécution de la peine (let. e); cinq ans après le paiement d'une peine pécuniaire ou après la cessation d'un travail d'intérêt général (let. f); ou dix ans après la fin de l'interdiction d'exercer une activité, de l'interdiction de contact ou de l'interdiction géographique au sens des art. 67 et 67b CP (let. l).

899 Cependant, en vertu de l'alinéa 2, dans les cas visés aux let. c et d, si l'acquittement ou le non-lieu est prononcé pour cause d'irresponsabilité de l'auteur, le profil d'ADN n'est pas effacé.

900 Dans le cadre de la procédure pénale suisse, il faut s'intéresser de plus près aux cas visés par l'art. 16 al. 1 let. a et c Loi sur les profils d'ADN. Afin de respecter les exigences de la jurisprudence nationale et internationale[788], la destruction d'un profil d'ADN doit intervenir en tout cas dès que la personne en cause ne peut être l'auteur de l'infraction.

---

[787] CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, § 70 ss.

[788] ATF 124 I 80, 84 = JdT 2000 IV 24, 27-28; TF 1C_51/2009 du 26 février 2009, c. 3.1; CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, § 114 ss.

901 En cas d'acquittement ou de non-lieu, la destruction doit intervenir dès l'entrée en force de la décision d'acquittement et un an après celle du non-lieu. Cette disposition est claire. Néanmoins il faut relever que, dans le CPP, la notion de non-lieu est inexistante et seul subsiste le classement.

902 En cas de classement (art. 319 ss CPP) ou de décision de non-entrée en matière (art. 310 CPP), la base légale de la Loi sur les profils d'ADN ne fournit pas clairement de réponse. La Cour européenne a considéré que la conservation de profils d'ADN après un classement s'inscrivait en violation de l'art. 8 CEDH[789]. En droit suisse, le classement intervient généralement dans les hypothèses où, si l'affaire devait être jugée, l'acquittement serait prononcé (art. 319 let. a à d CPP). Le classement peut donc être assimilé à un acquittement (dans ce sens: art. 320 al. 4 CPP). Par conséquent, en cas de classement, la destruction du profil d'ADN doit intervenir immédiatement après l'entrée en force de la décision, comme l'art. 16 let. c Loi sur les profils d'ADN le prévoit explicitement pour l'acquittement.

903 Au surplus, en tout hypothèse, est néanmoins réservée l'application de l'alinéa 4. Les profils d'ADN qui ne sont pas effacés en vertu de l'art. 16 al. 1 Loi sur les profils d'ADN le sont d'office après trente ans. La réserve de l'alinéa 4 concerne uniquement les profils d'ADN lorsqu'un auteur purgeant une peine privative de liberté est interné ou se voit appliquer une mesure thérapeutique. L'effacement de son profil intervient alors vingt ans après la libération de la peine privative de liberté ou l'internement, ou encore après la fin de la mesure thérapeutique.

904 A noter que l'approbation de l'autorité judiciaire est demandée dans les cas où l'effacement du profil d'ADN entre dans les cas visés par l'art. 16 al. 1 let. e et f et al. 4 Loi sur les profils d'ADN. Il n'est pas exclu que l'effacement soit refusé si un soupçon existe quant à la commission d'un crime ou d'un délit non prescrit ou si un risque de récidive existe.

905 Quant au profil d'ADN établi à partir d'une trace indiciale, l'art. 18 Loi sur les profils d'ADN instaure l'effacement: à la demande de l'autorité qui a ordonné la mesure sitôt que les traces peuvent être attribuées à une personne dont il est exclu qu'elle soit l'auteur du crime ou du délit, ou d'office après trente ans, sauf en cas de crime imprescriptible.

[789] CourEDH, Affaire *T. c. Royaume-Uni*, arrêt du 16 décembre 1999, 24724/94, § 75 et 85; CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, § 125.

2. L'identification judiciaire

906 Actuellement, l'opinion publique et les positions politiques s'axent notamment sur une volonté d'ordre public, conséquemment de répression de la criminalité. Pour lutter efficacement, le profilage ADN fournit un élément identificatoire vraisemblablement fiable et dénué de subjectivité ou d'arbitraire.

907 Corrélativement à ce qui prévaut pour la preuve dactyloscopique[790], le profil génétique est largement apprécié par les tribunaux grâce à sa nature scientifique et son objectivité[791]. Le mode d'énonciation du résultat et la valeur probante de l'identification par l'ADN mérite quelques explications.

a. La nature scientifique et identificatrice de l'ADN

908 Les données génétiques extraites de l'ADN sont une large source d'informations sur les individus. Une analyse de cette macromolécule permet de connaître l'état de santé d'une personne, notamment d'appréhender les maladies héréditaires[792]. Les informations tirées de l'analyse permettent en outre d'établir la filiation ou servent d'élément de preuve lors de la commission d'un acte délictuel.

909 En étant immuable, inaltérable et unique, l'ADN offre un potentiel d'identification pratiquement – les jumeaux homozygotes ayant le même ADN – comparable à celui des empreintes digitales[793]. Il peut servir à identifier un potentiel coupable, à écarter l'implication d'un innocent, voire à identifier la victime, ou plus spécifiquement à fournir une probabilité quant à l'identification de ces personnes.

910 L'apport de l'ADN et du profilage génétique n'est plus à prouver dans le cadre de la procédure pénale. Les qualités fondamentales de l'ADN et la possibilité d'effectuer un traitement automatisé pour établir et comparer les profils ADN renforcent le succès de l'usage de cette macromolécule.

---

[790] Supra Partie II, Chapitre 2, I, B, 2, n° 610 ss.

[791] A ce sujet: KLUMPE, p. 265.

[792] ROHMER, Thèse, p. 35; VUILLE, Thèse, p. 53 et 150.

[793] ESCONDIDA, TIMÉLOS, p. 2; KILLIAS, HAAS, TARONI, MARGOT, p. 297.

b. La nature probabiliste de la preuve

911 L'analyse génétique à des fins d'identification est un examen comparatif de deux ou plusieurs profils génétiques impliquant un pouvoir discriminatoire. Cependant, la discrimination n'est pas absolue. Les techniques d'identification génétique ne faisant pas appel à l'intégralité de l'ADN mais à un certain nombre de segments, deux profils peuvent être liés à une trace alors même que l'ADN dans son intégralité est unique.

912 Alors que la science reconnaît qu'il est possible de rejeter de manière absolue la concordance, le résultat identificatoire positif ne peut être fourni que sous terme de probabilité[794].

i. La théorie de la coïncidence fortuite et la population de référence

913 L'aptitude identificatoire d'un marqueur génétique est proportionnelle à son polymorphisme présentant la particularité d'être discriminatoire. Ainsi, l'analyse ADN suggère une étude marqueur par marqueur pour exclure les coïncidences fortuites dans la concordance des profils[795].

914 L'estimation de la fréquence d'apparition de chaque allèle dans une population de référence – déterminée sur la base des circonstances du cas d'espèce et constituée du groupe d'individus auquel le véritable auteur appartient – est le point central pour déterminer si les marqueurs choisis sont suffisamment discriminants afin de fournir un résultat identificatoire probant[796]. Ainsi, la "probabilité d'identité" déterminant le pourcentage que deux individus possèdent le même allèle est réalisé pour chaque marqueur.

915 Par une simple formule mathématique, il est possible d'obtenir la probabilité finale de la correspondance fortuite, soit la fréquence d'apparition de la caractéristique génétique dans une population de référence. Plus elle s'approche de 0%, meilleure est l'unicité des marqueurs analysés[797].

916 Dans le cadre juridique, la probabilité de coïncidence fortuite n'est cependant pas satisfaisante pour évaluer la valeur probante de la preuve génétique. Le juge ne désire pas uniquement connaître le pourcentage de coïncidence, il veut également déterminer la

[794] ESCONDIDA, TIMÉLOS, p. 4; KÖLLER, NISSEN, RIESS, SADORF, p. 2.

[795] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 75 et 78-84; HUYGHE, ADN, p. 19; KLUMPE, p. 23.

[796] OPECST, ADN, p. 55; TARONI, preuve ADN, p. 284; VUILLE, Thèse, p. 141.

[797] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 311 ss.

probabilité que la trace provienne de l'accusé. En outre, la formulation du résultat peut induire le juriste en erreur.

917 Admettons que, suite aux calculs, la coïncidence fortuite est de 2%, la conclusion risque fort d'être que "l'ADN de la trace relevée sur les lieux et l'ADN du suspect concordent à 98%, soit il n'existe que 0,02 chance que l'auteur de la trace soit une autre personne" – thèse défendue vraisemblablement par l'accusation –, ou "la population d'intérêt étant de 400'000, 8'000 personnes présentent la même caractéristique diminuant à 1/8'000 la chance que le suspect soit l'auteur" – thèse défendue par la défense[798].

918 Aucune de ces deux conclusions n'est correcte.

919 La première fournit à la Cour une affirmation que le suspect est la source de la trace et ne se focalise pas sur la valeur du profil génétique. *In casu*, il omet de tenir compte de la population d'intérêt et donc de la possibilité qu'une autre personne soit auteur de la trace.

920 La seconde, par l'avance de chiffres fictifs, transforme la probabilité. Même si la logique de l'avocat est parfaitement juste, il n'est pas rare que la taille de la population proposée soit trop élevée pour affaiblir la valeur probatoire de l'analyse génétique, ce qu'on nomme communément "*Defense Attorney's Fallacy*"[799].

921 La présentation des résultats identificatoires grâce aux calculs de la coïncidence fortuite n'est donc pas adéquate lors d'un procès pénal. En effet, les chiffres avancés ne sont pas pertinents, mais soumis à la subjectivité de deux argumentations extrêmement différentes. Ensuite, la présentation des résultats sous cette forme n'a pas de sens lorsque le suspect est un proche parent de la source de la trace indiciale[800]. Il est important de ne pas perdre de vue que l'analyse de comparaison génétique sous forme de probabilité est une information indirecte qui doit être combinée avec d'autres éléments pour permettre l'estimation correcte de ce qu'elle démontre, notamment en prenant en compte la fréquence du groupe sanguin ou en faisant évoluer les chances accordées à l'existence d'un fait, et ne doit, en aucun cas, être soumise à une pure interprétation subjective[801].

---

[798] CHAMPOD, TARONI, RPS 1993, p. 227; TARONI, preuve ADN, p. 285-286; TARONI, MANGIN, BÄR, p. 440-441.

[799] CHAMPOD, TARONI, RPS 1994, p. 203; RODRIGUEZ, p. 26; VUILLE, Thèse, p. 196-197.

[800] TARONI, LAMBERT, FEREDAY, WERRETT, p. 24-26; VUILLE, Thèse, p. 145.

[801] CHAMPOD, TARONI, RPS 1994, p. 201; TARONI, preuve ADN, p. 288.

ii. Le rapport de vraisemblance et le modèle bayésien

922 Pour éviter les pièges liés à l'intuition, les anglo-saxons ont défini la place de l'indice matériel dans le procès pénal comme un indice qui a une influence, lors de l'appréciation par le juriste, sur la culpabilité[802].

923 Le théorème de Bayes exploitant le rapport de vraisemblance – *"Likelihood Ratio"* (LR)[803] – décrit de manière correcte la valeur probatoire de l'identification génétique dans le contexte des faits à juger. Le modèle bayésien combine des informations *a priori* et *a posteriori* sur l'existence et l'inexistence d'un fait[804].

924 Traduite dans le contexte de la preuve génétique par l'ADN, la théorie bayésienne résout le passage entre les chances accordées par le juriste à la thèse de culpabilité du suspect avant l'apport de l'élément scientifique et les nouvelles chances accordées par ce même juriste après l'apport de la preuve ADN. Ces dernières sont le résultat de la multiplication des premières chances par un rapport LR qui se traduit comme le rapport entre la probabilité de retrouver l'élément de preuve dans l'hypothèse où le suspect est à l'origine de la trace et la probabilité de retrouver cet élément dans l'hypothèse où le suspect n'est pas à l'origine de la trace[805].

925 Prenons un exemple: préalablement à l'expertise ADN, le juge considère les chances que le suspect soit innocent à 10 contre 1; l'expertise établit un lien entre la trace et le suspect, la probabilité est de 1, soit 100%; la fréquence d'apparition de ce caractère dans la population considérée est de 2%. Le LR obtenu est de 50, ce qui augmente de 50x les chances que le suspect soit coupable. L'apport de l'indice matériel fait passer les chances à 5 contre 1.

926 Le théorème de Bayes est complexe pour un juriste puisqu'il fait appel à des connaissances en mathématique relativement poussées. Cependant, il permet de démontrer qu'une identification n'est pas noire ou blanche et limite l'expertise qui démontre uniquement si le suspect a pu ou non laisser une trace et dans quelle mesure cette possibilité existe[806], sans jugement de culpabilité ou d'innocence.

---

[802] CHAMPOD, TARONI, RPS 1993, p. 227; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 317-325; MANGIN, TARONI, p. 507.

[803] A ce sujet, voir: VUILLE, Thèse, p. 146-148.

[804] BÄR, p. 43; EVETT, p. 121; KÖLLER, NISSEN, RIESS, SADORF, p. 18; SCHWEIZER M., p. 172; TARONI, AITKEN, p. 294-295 et 300; TARONI, MANGIN, BÄR, p. 442; VUILLE, TARONI, RPS 2011, p. 170-171.

[805] CHAMPOD, TARONI, RPS 1993, p. 228; CHAMPOD, TARONI, RPS 1994, p. 211; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 317-318; KÖLLER, NISSEN, RIESS, SADORF, p. 20 et 23-24; OPECST, ADN, p. 55-56.

[806] BÄR, p. 45 et 50; KLUMPE, p. 29; MANGIN, TARONI, p. 507; TARONI, MANGIN, BÄR, p. 444.

927 Ainsi, le résultat obtenu prend en considération la non-unicité d'un profil d'ADN, évite que seule la probabilité liée à la coïncidence fortuite influe sur la culpabilité ou l'innocence, exclut que des interprétations subjectives s'immiscent dans la preuve scientifique et laisse le juge seul compétant pour évaluer les chances *a priori* et *a posteriori*.

c. La valeur probatoire

928 Scientifiquement, la valeur de l'analyse comparative génétique et l'identification possible qui s'en suit reposent sur le caractère objectif des résultats mathématiques, méthodiques et logiques ainsi que sur la force acquise par les développements de la science dans le domaine de l'ADN avec la concrétisation de sa fiabilité à travers les années.

929 Plus précisément, l'idée de reconnaissance d'un individu par son ADN repose sur la découverte de l'individualité génétique – exception faite des jumeaux homozygotes –, la pérennisation et l'inaltérabilité de la molécule ADN, soit sur des principes théoriques. Ainsi, dépendamment de l'état du matériel génétique comparé, du nombre de marqueurs analysés et de leur pouvoir discriminant, l'ADN semble offrir de larges perspectives d'identification grâce à l'addition des observations réalisées[807].

930 Conséquemment, la valeur probatoire de l'identification ADN reconnue par les scientifiques est forte et indiscutable donnant l'illusion d'apporter la vérité, vision partagée par les juristes[808].

931 En Suisse, la question de l'admissibilité de la preuve génétique est laissée à la libre appréciation des juristes. Encore faut-il que le juge comprenne les éléments probatoires et les interprète correctement[809]. La génétique étant une science requérant des connaissances spécifiques, les experts en sciences forensiques sont régulièrement sollicités pour éclairer la Cour sur les questions d'ordre technique.

932 Théoriquement, le juge du fond est libre de réfuter ou non, dans le contexte de l'affaire, la preuve apportée. Dès lors, la valeur probante du profilage ADN et l'identification subséquente ne devraient pas être automatiques, ni liées directement à la reconnaissance scientifique de la fiabilité de l'analyse génétique.

---

[807] COQUOZ, p. 166; HUYGHE, ADN, p. 49.

[808] DONATSCH, RPS 1991, p. 179; FRANCILLON, p. 144; HAURI, p. 403; HAUSER, SCHWERI, HARTMANN, p. 311; PADOVA, p. 72-73; ROHMER, Thèse, p. 125.

[809] HAURI, p. 405; TARONI, preuve ADN, p. 276.

933 En d'autres termes, le juge du fond doit examiner la preuve matérielle par l'ADN et avoir un regard critique sur l'expertise à la lumière de la source du matériel biologique, de la méthode utilisée pour l'analyse, des moyens probabilistes avancés, des étapes d'interprétation des résultats, des risques d'erreurs, de la qualification de l'expert, etc.[810]. Pourtant, à la lecture de la jurisprudence, il est fort de constater que le Tribunal fédéral fixe un seuil de doute raisonnable pour reconnaître une valeur au profilage ADN.

934 En matière de test de paternité – utile notamment pour relier une trace inconnue ou identifier un cadavre –, le seuil est clairement défini tant pour la probabilité *a priori* que celle *a posteriori*, ce dernier devant s'élever à 99,8% revenant à exiger un LR d'au minimum 500[811]. Dans le cadre pénal, la réflexion est plus complexe puisque, bien souvent, la probabilité *a priori* est très faible impliquant que le LR soit très fort nécessitant une fréquence de similitude d'ADN très faible pour reconnaître une valeur à la probabilité *a posteriori*[812].

935 Même si ces limites ou règles non-contraignantes ont l'avantage de fixer un cadre à l'acceptation et à la prise en compte de l'identification génétique, elles omettent l'intégration du facteur humain qui peut influer sur les résultats et leur perception. En l'espèce, fixer un seuil de doute raisonnable est insuffisant pour déclarer qu'une preuve est fiable ou non. Il est impératif que l'évaluation de la valeur probatoire prenne en considération les risques, contaminations ou autres circonstances qui peuvent influer sur la qualité de la preuve biologique, intègre la preuve à la lumière du cas d'espèce, et ouvre un réel débat sur l'appréciation de la preuve par l'ADN.

936 Dans les jugements publiés jusqu'ici, le constat est sans appel, une présentation concise du moyen de preuve génétique est effectuée, mais l'examen de la valeur probatoire se résume à tenir compte de la pure valeur scientifique et de l'évaluation effectuée par l'expert sans plus de débat. Pourtant, en criminalistique, le résultat d'une comparaison ADN ne se résume guère en l'affirmation ou la négation de l'identification, les juristes doivent s'interroger sur l'expérience du scientifique et la combinaison des éléments d'interprétation entre le calcul probabiliste et la conclusion émise[813]. Ce n'est qu'avec une réelle discussion durant le procès que la crédibilité de l'expertise peut être reconnue et, conséquemment, que la force probante de l'identification génétique dans l'état de fait se construira.

---

[810] HAURI, p. 405.

[811] ATF 101 II 13, 15.

[812] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 320-321; VUILLE, Thèse, p. 151-152.

[813] CHAMPOD, TARONI, RPS 1993, p. 225; EVETT, p. 121; VUILLE, Thèse, p. 347-348.

937 En outre, la preuve génétique n'est pas une preuve de culpabilité ou d'innocence en soi. Si, par exemple, du matériel ADN est découvert sur les lieux de l'infraction et qu'après comparaison une identification est réalisée, cela ne signifie pas encore que l'individu à la source de la trace est l'auteur de l'acte délictuel. L'analyse génétique n'est qu'une présomption que le profil génétique indicial appartient à une personne déterminée, mais en aucun cas elle ne donne un résultat identificatoire certain, ni quant aux circonstances de la présence de ce matériel biologique sur la scène de crime[814].

938 Ainsi, le "hit" entre un individu et une trace n'est qu'un indice qu'il faut intégrer correctement dans le faisceau de preuves nécessaire à l'obtention de l'intime conviction ou, au contraire, à la constatation qu'un doute raisonnable subsiste[815].

939 En conséquence, la preuve par l'ADN n'est pas probante sans examen approfondi de sa pertinence. Le juge ne doit pas perdre de vue que, malgré la fiabilité de la génétique, la quantité d'ADN, le degré de dégradation, la présence de substances interférentes, la présentation des résultats par l'expert, la compréhension des résultats probabilistes et les raisons expliquant la présence de l'ADN de l'individu identifié sur les lieux de l'infraction limitent la "vérité" découlant de l'analyse génétique. Dès lors, la preuve génétique doit intervenir en complément d'autres investigations et appréciations probatoires.

C. La discussion sur la preuve génétique

940 Conceptuellement, l'analyse ADN est similaire aux autres preuves indiciales, elle fait suite à la recherche de traces, leur récolte et leur interprétation à la lumière du cas d'espèce. Concrètement, sa reconnaissance scientifique fait de ce moyen de preuve une valeur "sûre" pour l'identification judiciaire, le plaçant au-dessus de certains autres types d'indices. L'engouement de la justice pour la preuve génétique s'explique par l'objectivité de la science et par les qualités, notamment identificatrices, reconnues à l'ADN. Cependant, la justice et ses acteurs ne doivent pas se réfugier derrière une image schématique de la preuve ADN en alléguant l'infaillibilité et la certitude de ce mode probatoire. Certes, l'identification génétique comporte un certain nombre de qualités qui font sa force, mais la justice doit conserver son esprit critique et ne pas perdre de vue certains facteurs pouvant réduire l'"absolue" vérité fournie par l'ADN.

---

[814] ANCEL, p. 202-203; BOURGEAULT, p. 116; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 324-325; JOBARD, SCHULZE-ICKING, p. 61; KILLIAS, HAAS, TARONI, MARGOT, p. 296; KLUMPE, p. 269; Polizeiliche Ermittlung-VOSER, p. 379; ROHMER, Thèse, p. 127.

[815] TF 6B_667/2007 du 16 février 2008, c. 3.2.2; ANCEL, p. 143; ESCONDIDA, TIMÉLOS, p. 12.

941 La présente partie doit permettre de fournir des pistes de réflexion aux juristes pour appréhender la preuve par l'ADN avec discernement et lucidité. Ainsi, en identifiant les points forts et faibles de cette preuve scientifique et en relevant les risques liés à son exploitation, chaque profane devrait pouvoir comprendre et discuter les enjeux de l'ADN en procédure pénale, extensivement déterminer la réelle valeur probatoire sans se référer aveuglément à la valeur scientifique.

1. L'évaluation de la preuve génétique dans l'ordre juridique suisse

a. Le potentiel de la preuve génétique

i. Les qualités scientifiques de la preuve par l'ADN

942 A l'image de la preuve dactyloscopique[816], la preuve génétique repose sur une science reconnue par le monde scientifique, sur le postulat que le profil génétique est individuel et se caractérise par sa nature hybride ainsi que par le potentiel probatoire à charge ou à décharge. La triple caractéristique de l'ADN – unicité, pérennité et inaltérabilité –, la reconnaissance scientifique de la génétique et les qualités liées à la nature scientifique de la preuve dactyloscopique – applicable en grande partie par analogie à la preuve génétique – ayant fait l'objet d'exégèses étendues[817], nous ne reviendrons que brièvement sur ces points favorables.

943 Les avancées de la recherche en matière de génétique humaine avec pour point d'orgue la découverte de l'individualité de l'empreinte génétique ont eu pour conséquence l'intégration de cette science et de ces possibilités identificatoires lors du procès pénal[818]. Il est indéniable que les possibilités d'identifier une personne isolée grâce à son patrimoine génétique est une des grandes forces de certitude de la preuve ADN; ce d'autant que les années de pratique scientifique ne sont pas illustrées par des erreurs ou contradictions, contrairement aux années de pratiques judiciaires de ce moyen probatoire comme nous le verrons ci-après[819]. La preuve génétique en tant que preuve découlant d'une science a le mérite d'exister par elle-même et ne nécessite pas de concrétisation.

---

[816] Supra Partie II, Chapitre 2, I, A, 2, n° 530 ss; Supra Partie II, Chapitre 2, I, B, 2, b, n° 624 ss; Supra Partie II, Chapitre, 2, I, C, 1, a, ii, n° 644 ss.

[817] Supra Partie II, Chapitre 2, I, A, 1, n° 592; Supra Partie II, Chapitre 2, I, C, 1, a, i. à iii, n° 639-653; Supra Partie II, Chapitre 2, II, A, 3, n° 813 ss.

[818] COQUOZ, p. 163; HUYGHE, ADN, p. 8; ROHMER, Thèse, p. 63; WERRETT, p. 21.

[819] Infra Partie II, Chapitre 2, II, C, 1, b, n° 974 ss et 996 ss.

944 L'ADN est individuel parce que sa constitution influencée par l'hérédité est telle qu'il est impossible d'obtenir deux empreintes identiques, c'est une certitude qui découle de la nature même du monde sans influence d'acteurs humains. La seule faiblesse de cette preuve scientifique revient donc seulement à la phase de comparaison qui relève d'une interprétation, non pas de la science, mais des résultats obtenus[820]. Néanmoins, en tant que preuve hybride, la phase plus subjective de comparaison de l'identification ADN est contrebalancée par l'objectivité de la science et le respect des règles de l'art par l'expert.

945 Ainsi, sa mixité subjective et objective permet à la preuve génétique de s'intégrer au procès pénal en faisant parler des indices qui, sans expertise, resteraient muets alors même qu'ils apportent une pierre précieuse à l'édifice de la décision juridique et fournissent une information avec une valeur nettement supérieure à celle d'un témoignage[821].

946 Au surplus, la preuve ADN étant une preuve identificatoire, selon le résultat obtenu, elle appuie soit la thèse de la défense concernant l'innocence de l'accusé, soit les allégations de l'accusation quant à la culpabilité de ce dernier. Ainsi, le profil génétique a une double finalité, elle peut soutenir l'intime conviction du juge qui rend une décision de culpabilité, si d'autres indices convergent dans ce sens ou, en cas de doutes ou d'exclusion de l'implication de l'accusé dans la commission de l'acte délictuel, elle peut servir à maintenir l'innocence et à amener le juge à rendre une décision d'acquittement[822].

ii. Les atouts du matériel génétique analysable

947 L'utilisation des profils génétiques en procédure pénale comporte plusieurs atouts, notamment quant aux caractéristiques de l'échantillonnage. L'ADN étant similaire dans toutes nos cellules, du matériel génétique de nature différente même en infime quantité peut être comparé à des fins identificatoires. Ainsi, grâce à la variété des sources d'échantillonnage et à l'amplification PCR, les possibilités identificatoires par l'ADN sont extrêmement importantes influant sur le succès des analyses génétiques en criminalistique et dans le cadre juridique. En sus, la molécule d'ADN est stable et perdure dans le temps[823]. Ainsi, un prélèvement effectué sur une preuve datant d'une dizaine d'années ou un échantillon

[820] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 236 ss; MATELLY, p. 121 ss.

[821] Supra Partie II, Chapitre 1, I, B, 1, a, n° 393 ss; Supra Partie II, Chapitre 1, I, C, n° 420 ss.

[822] ANCEL, p. 143; BURR, p. 176 et 178; DURUPT, p. 76-77; ESCONDIDA, TIMÉLOS, p. 15-16; FRANCILLON, p. 144; JOBARD, SCHULZE-ICKING, p. 44; LEMAN-LANGLOIS, BRODEUR, p. 74; MANAOUIL, WERBROUCK, TRAULLE, CORDIER, GIGNON, JARDE, p. 20; PIQUEREZ, Traité de procédure pénale suisse, p. 500; ROHMER, Thèse, p. 125-126.

[823] Supra Partie II, Chapitre 2, II, A, 3, n° 813-817.

correctement conservé depuis une centaine d'années n'exclut pas l'établissement du profil génétique de l'individu, ni de la comparaison subséquente.

948 Pour le criminaliste, la durée de vie d'une trace ou d'un échantillon d'ADN n'est pas d'une grande importance, puisque soit elle existe soit elle n'existe pas, extensivement soit l'analyse est possible soit non. En revanche, à des fins probatoires, la longévité a plusieurs intérêts. Premièrement, elle permet d'élargir les possibilités d'analyses comparatives, notamment en rouvrant de manière systématique les affaires criminelles non élucidées ou en offrant la possibilité d'effectuer une contre-expertise[824]. Deuxièmement, l'état de la trace peut influer sur ce qu'elle démontre et sa force de conviction. Il faut cependant souligner que les techniques d'analyse ne permettent pas de dater dans le temps l'âge d'une cellule, la durée n'est donc pas probante pour "*déterminer à quel moment, antérieur, concomitant ou postérieur [à l'acte délictuel] les traces ont été laissées*"[825].

949 En outre, si les caractéristiques de l'échantillon d'ADN et sa longévité permettent une lutte efficace contre la criminalité, la partie codante peut fournir des informations sensibles sur les individus concernés qui ne sont pas utiles à cette lutte[826]. Pour parer à la mise en péril de la liberté personnelle et du droit à l'autodétermination informationnelle, l'échantillon utilisé pour établir le profil génétique doit se cibler sur la partie non-codante de l'ADN (art. 2 al. 1 Loi sur les profils d'ADN), partie ne contenant pas de données sensibles, avec pour exception l'analyse du sexe[827]. En effet, les types de maladies ou les caractéristiques héréditaires ou génétiques n'intéressent pas la justice qui cherche à identifier un potentiel coupable[828]. En se limitant à la partie de l'ADN ne comportant pas d'informations relatives à la psychologie ou à la physiologie de la personne, l'identification n'en est pas moins possible, ce qui renforce l'attrait de la justice pour cette preuve évitant ainsi les atteintes non-nécessaires et/ou non-proportionnées aux droits fondamentaux car sans utilité pour l'identification et/ou trop invasives.

[824] ANCEL, p. 144; OPECST, ADN, p. 57.

[825] Cour de cassation, 01-85.386, c. 5.

[826] GEHRIG, LAHARPE, p. 1801-1807; ROHMER, Thèse, p. 99 et 352.

[827] BURR, p. 104; COQUOZ, COMTE, HALL, HICKS, TARONI p. 417-419.

[828] ANCEL, p. 218; BUSCH, p. 637.

iii. L'assurance de qualité de l'expertise

950 Le Département fédéral de justice et police a édicté une ordonnance sur les exigences requises pour les laboratoires forensiques d'analyse d'ADN[829] complétant l'art. 2 al. 2 Ordonnance sur les profils d'ADN.

951 Le respect des exigences légales devant être remplies par les laboratoires doit assurer la bonne exécution des analyses. Pour ce faire, un organe externe vérifie qu'une formation adéquate et continue est suivie par les experts en ADN, que les méthodes d'analyses utilisées sont validées et fiables, et que les tests de performance ont été passés avec succès. La certification des laboratoires a été instaurée dans le dessein de reconnaître et de garantir une certaine qualité aux analyses ADN effectuées, c'est-à-dire que la trace biologique soit correctement prélevée, que l'établissement du profil génétique soit réalisé dans les règles de l'art et que l'interprétation fournie par les experts soit juste et professionnelle.

952 Conséquemment, le modèle d'accréditation des laboratoires choisi par la Suisse conditionne une certaine force de conviction, le juge pouvant se reposer sur le professionnalisme des experts, leurs compétences et leur indépendance institutionnelle[830]. De plus, ce modèle a l'avantage de laisser une certaine marge de liberté aux magistrats lors du choix de l'expert, puisque ce n'est pas lui, personnellement, qui doit être autorisé, mais le laboratoire pour lequel il travaille.

iv. La nature probabiliste des résultats d'expertise

953 Dès lors que l'expert se base sur une partie de l'ADN et ses capacités discriminatoires pour fournir un résultat, l'individualité du matériel biologique découvert sur les lieux de l'infraction ou sur des objets y afférant ne peut se concevoir qu'en terme statistique[831]. En effet, les statistiques prennent en considération notamment le taux d'erreur et l'estimation de l'impact des événements incertains. Contrairement à la preuve dactyloscopique présentée univoquement, la preuve génétique s'exprime donc par une probabilité pouvant être accompagnée d'un avis qualifié de l'expert. Ce mode d'administration de la preuve

[829] Ordonnance du DFJP sur les exigences de prestations et de qualité requises pour les laboratoires forensiques d'analyse d'ADN du 8 octobre 2014 (Ordonnance du DFJP sur les laboratoires d'analyse d'ADN), RS 363.11.

[830] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 443-444; NATIONAL RESEARCH COUNCIL, p. 195; SCHWEIZER M., p. 175; VUILLE, Thèse, p. 151-152.

[831] ALTENDORFER, p. 48; BURR, p. 32-33; RODRIGUEZ, p. 23; TARONI, preuve ADN, p. 279.

scientifique a le grand avantage de prendre en considération la réalité de l'analyse comparative sans pallier l'insuffisance d'une preuve[832].

954 Les informations forensiques et leur interprétation impliquent des subtilités scientifiques difficiles à appréhender pour les juristes. Grâce à l'approche bayésienne comme méthode probabiliste, la preuve scientifique, *in casu* l'identification génétique par l'ADN, est abordée de manière adéquate et viable par l'évaluation d'une paire d'hypothèses. Cette approche correspond clairement au processus judiciaire où l'hypothèse de l'accusation et de la défense se confrontent. Ayant au départ chacune une certaine probabilité d'être vraies, l'examen probabiliste de l'analyse ADN modifie l'une ou l'autre des probabilités *a priori* – soit pour la conforter soit pour l'affaiblir – et ainsi fournit un rapport de vraisemblance qui vient éclairer le tribunal dans l'évaluation concrète et objective des faits. En d'autres termes, la théorie de Bayes souligne les questions auxquelles le scientifique doit répondre, notamment celle de savoir dans quelle mesure l'indice soutient la thèse de la défense ou de l'accusation, sans dire si oui ou non l'accusé est l'auteur de la trace biologique découverte[833]. Ainsi, l'expert et le juge se positionnent correctement dans le cadre de l'appréciation de la preuve. Le scientifique évalue le rapport de vraisemblance et le juge apprécie les chances *a priori* et *a posteriori*[834].

955 En conséquence, la théorie d'interprétation par le théorème de Bayes ne laisse pas l'exclusivité à un chiffre final donné par l'expert, mais positionne correctement l'indice dans sa démonstration permettant à la valeur probatoire de se dégager objectivement et d'être évaluée en lien avec une nouvelle information et dans le cas d'espèce à juger.

b. Les problématiques liées à l'exploitation et à l'administration de la preuve génétique

i. L'unicité relative du profil génétique

a) Le cas des vrais jumeaux

956 Le postulat que l'ADN est propre à chaque être humain doit être nuancé. Même s'il est presque unanimement reconnu que chaque individu a son propre ADN, l'ADN des jumeaux

[832] CHAMPOD, TARONI, RPS 1994, p. 204; RODRIGUEZ, p. 23; TARONI, MANGIN, BÄR, p. 442 et 444.

[833] ANTOGNINI, p. 13; BÄR, p. 50-51; CHAMPOD, TARONI, RPS 1993, p. 235; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 317-318; HUYGHE, ADN, p. 50-51; TARONI, AITKEN, p. 302-303.

[834] DONATSCH, Jusletter, n° 10-15; OPECST, ADN, p. 56; VUILLE, TARONI, forumpoenale, p. 367.

homozygotes fait exception[835]. Etant issus d'une fécondation d'un même ovule avec un spermatozoïde et la division en deux foetus ayant lieu après la répartition des génomes paternel et maternel pour former le génome de l'embryon, leur patrimoine génétique est rigoureusement identique, extensivement leur profil d'ADN ne peut qu'être semblable.

957 A l'exception des jumeaux homozygotes, nous pouvons vraisemblablement admettre qu'aucun être humain n'a le même ADN. Cependant, il n'est pas exclu que le profil d'ADN d'une personne soit similaire à celui d'un autre individu[836].

b) Le cas des coïncidences fortuites

958 Les experts n'excluent pas la possibilité d'obtenir ce qu'ils nomment des "*coïncidences fortuites*"[837], c'est-à-dire la concordance de deux profils alors même que l'individu identifié n'était pas présent sur les lieux, n'avait eu aucun contact avec la victime et n'avait jamais touché de près ou de loin un objet pouvant se rapporter à l'acte délictuel.

959 Même si l'examen d'ADN effectué indique une probabilité infime de trouver deux profils d'ADN identiques, il n'est pas impossible que tel soit le cas. En effet, l'analyse ADN s'effectue sur une fraction de la molécule. Si les différences entre le profil d'ADN de la trace et de l'individu faussement identifié se situent sur des zones non-choisies pour être des marqueurs, elles n'apparaissent pas sur le profil d'ADN et les deux profils peuvent alors être semblables.

960 Pour limiter au maximum les risques de coïncidence fortuite, le nombre de marqueurs analysés joue un rôle. Plus ce nombre est grand, plus les chances de discriminer des individus augmentent[838].

961 La problématique des analyses effectuées au sein d'une population relativement fermée marque l'importance du nombre de marqueurs à comparer[839], sans toutefois nécessiter une analyse intégrale de l'ADN qui serait irréaliste financièrement et sous l'angle de la rentabilité. Dans ce type de population de référence, la fréquence d'apparition d'un caractère identique

---

[835] BUQUET, p. 177; HUYGHE, ADN, p. 18; KILLIAS, HAAS, TARONI, MARGOT, p. 296; MALAUZAT, p. 73; MARGOT, CHAMPOD, p. 239; ROHMER, Thèse, p. 48; ROUX, p. 180; SCHMID, Handbuch, p. 470.

[836] ANCEL, p. 155; CHAMPOD, TARONI, RPS 1993, p. 226; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 109 et 303-304; ROHMER, Thèse, p. 126; ROUX, p. 181; SCHWEIZER M., p. 173-174.

[837] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 429-430; RUCKSTUHL, DITTMANN, ARNOLD, p. 249.

[838] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 313; KNOPPERS, GRIMAUD, CHOQUETTE, LE BRIS, p. 62.

[839] ANCEL, p. 155-156; COQUOZ, TARONI, p. 271; HENNAU-HUBLET, p. 39; KÖLLER, NISSEN, RIESS, SADORF, p. 25.

chez deux individus augmente considérablement, ce qui engendre des risques plus élevés de coïncidences fortuites, ce d'autant si l'ADN mitochondrial – semblable à tout individu ayant la même mère – est seul analysé.

962 Dans une optique de rentabilité et d'utilité des profilages génétiques, il est donc important d'analyser un nombre suffisant de marqueurs. Ce nombre doit varier en fonction du mélange ou de la consanguinité de la population de référence.

963 Relevons encore que l'évolution des bases de données recensant les profils d'ADN accentue le risque d'obtenir deux profils similaires. Même si le fichage privilégie et ne concerne que les profils établis à l'aide d'ADN nucléaire[840], ce n'est toujours qu'un fragment de l'empreinte génétique qui est analysé, n'excluant pas les similitudes. Plus la base de données comporte de profils d'ADN, plus le risque de coïncidences fortuites est élevé. Les scientifiques ne nient d'ailleurs pas que si nous comparions deux à deux tous les individus de la planète, il est quasiment certain de trouver des paires d'individus possédant le même profil[841].

964 Ces constations ont pour effet d'affaiblir la valeur probatoire de la preuve par l'ADN et renforcent l'usage nécessaire des probabilités lors d'identification judiciaire. En effet, il ne faut pas confondre unicité et rareté. L'intégralité de l'ADN est unique, alors que la découverte de deux profils d'ADN similaires est rare.

965 Pour écarter tout doute raisonnable quant aux coïncidences possibles et à la qualité polymorphe de ceux-ci, soit pour individualiser un profil d'ADN, les experts forensiques et la justice doivent considérer la quantité des marqueurs analysés et leur pouvoir discriminatoire[842]. L'examen de ces deux points permet d'évaluer correctement la certitude ou les risques consécutifs à l'analyse génétique sans considérer l'identification comme absolue.

c) Le cas des proches parents

966 Les rapports d'expertise spécifient fréquemment que le résultat probabiliste est fourni en lien avec une population de référence non apparentée. Ainsi, la probabilité résultant de l'analyse des profils d'ADN ne prend pas en considération le fait que le résultat de coïncidence fortuite est plus élevé entre proches parents.

---

[840] KILLIAS, HAAS, TARONI, MARGOT, p. 297.

[841] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 303.

[842] ANCEL, p. 156; HUYGHE, ADN, p. 19.

967 Dans les cas de population avec un fort taux de consanguinité, la prise en considération des personnes apparentées au suspect peut faire évoluer drastiquement le résultat probatoire. En ne prenant pas en compte une population de référence correcte, soit en ignorant les liens de parenté, une erreur se produit dans le résultat qui conduit à sous-évaluer la probabilité de coïncidences fortuites[843].

968 Plus il existe de proches parents du suspect dans la population de référence, plus il y a de chances que le suspect ne soit pas le seul à avoir un profil d'ADN qui correspond à la trace découverte.

969 Par conséquent, une erreur sur la population de référence fournit un pourcentage de concordance plus élevé que ce qu'il est en réalité. Ce constat marque l'importance de ne pas s'arrêter sur une probabilité de coïncidences fortuites et à développer la théorie bayésienne pour évaluer adéquatement la preuve apportée[844].

ii. Les risques d'erreurs liés à l'échantillon

970 Les analyses d'ADN se déroulent dans le monde réel et non dans un univers théorique. La pertinence et la fiabilité des éléments apportés par la preuve scientifique ne sont pas remises en question. En revanche, le facteur humain ou naturel peut influencer les résultats.

a) Le transfert d'ADN

971 Les cellules se déposent au gré des mouvements d'un individu ou du contact de sa peau avec un objet. Les traces de contact contiennent généralement une infime quantité d'ADN qui, parfois, est dégradé ou mélangé. Cependant, il n'est pas exclu qu'un bon donneur laisse un profil complet sur un objet qu'il a touché.

972 En cas de transfert primaire, la trace de contact peut être analysée et permettre d'obtenir un profil d'ADN. Néanmoins, comme pour toutes les traces génétiques, il est impossible de dater le moment du dépôt. Par conséquent, il est nécessaire de considérer tous les éléments mis à la disposition des autorités pénales.

[843] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 341-350; LEMPERT, p. 308-309; VUILLE, Thèse, p. 201.

[844] Supra Partie II, Chapitre 2, II, B, 2, b, n° 911 ss.

973 Alors qu'en soi les traces provenant d'un transfert primaire ne posent guère de difficulté, or cas où l'ADN serait très endommagé, le cas des traces de contact par transfert secondaire, voire tertiaire, ne sont pas à négliger[845]. Ainsi des cellules de peau d'une personne peuvent se retrouver sur une victime ou sur l'auteur d'une infraction par transfert, alors même que le donneur de ces traces de contact n'a pas côtoyé l'une ou l'autre de ces personnes.

974 L'affaire du taximan David Butler est l'un des dossiers le plus représentatif de la problématique du transfert[846]. Durant la nuit du 15 septembre 2005, Anne Marie Foy, une prostituée, est assassinée, battue à mort à l'aide de branche d'arbre. En 2005, es investigations n'ont pas permis d'identifier un suspect, mais dans le cadre d'une enquête du service des affaires classées, David Butler est suspecté en 2011.

975 La police scientifique anglaise a vérifié à nouveau l'ADN retrouvé sous les ongles de la victime. La première fois, en 2005, il n'y a eu aucun hit. Or, pour une raison indéterminée, la comparaison fournit un résultat avec un ADN retrouvé sur un mégot de cigarette dans le cadre d'une affaire de cambriolage au domicile de la mère de David Butler.

976 David Butler est alors accusé du meurtre d'Anne Marie Foy.

977 Cela étant, le processus d'analyse employé n'était pas convaincant. En effet, David Butler souffre d'une maladie asséchant de manière importante sa peau. Les collègues du suspect l'appellent même "le taxi feuilleté". Dès lors, il n'est pas impossible que le vrai coupable, puisque la victime n'a pas emprunté le taxi de David Butler, soit entré dans le taxi de David Butler et qu'un transfert d'ADN ait eu lieu.

978 Durant le procès de David Butler, plusieurs experts forensiques ont témoigné et ont démontré avec quelle facilité un ADN pouvait se transporter d'un point à un autre, alors même que la personne se trouve à plusieurs dizaines, voire centaine, de kilomètre. Ils ont également insisté sur le fait qu'aujourd'hui, les techniques permettent qu'une infime quantité soit retrouvée pour qu'une analyse arrive à un résultat positif.

979 La Cour anglaise a conclu que l'ADN retrouvé n'était pas déterminant et qu'en l'absence de faisceau d'indices, David Butler n'était pas coupable.

980 Ce constat nous mène à insister sur le fait qu'une preuve génétique ne démontre que la présence ou le contact entre l'auteur et un individu sans pouvoir déterminer les

[845] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 254-255; VUILLE, Thèse, p. 38.

[846] The Telegraphe, *The case against DNA*, article du 6 mars 2012.

circonstances ou le moment du dépôt de la trace. En somme, la découverte du profil d'ADN d'un individu ne signifie pas encore qu'il soit le coupable.

981 Bien plus encore, un cas de transfert à marquer les autorités britanniques, il s'agit de l'affaire Scott[847].

982 Le 23 octobre 2011, Adam Scott est accusé de viol par la police de Greater Manchester et placé en détention. Ladite police s'est basée sur une unique preuve, soit le profil ADN partiel faisant suite à une analyse génétique par le LGC Forensics dans le laboratoire de Teddington de ce qu'il croyait être un échantillon prélevé sur la victime d'un viol.

983 Cela étant, le téléphone mobile d'Adam Scott a été localisé, quelques heures après l'heure du viol, à Plymouth au sud de l'Angleterre alors même que le viol avait eu lieu à Manchester. Cette nouvelle preuve a incité la police de Greater Manchester a s'interrogé sur la validité du test ADN. C'est pourquoi, un expert a été nommé pour évaluer les circonstances du *hit*[848].

984 L'enquête d'Andrew Rennison a conclu au fait que l'échantillon d'ADN d'Adam Scott s'était trouvé par hasard analysé, mais ne faisait pas partie des échantillonnages prélevés sur la victime[849].

985 Ce qui s'est passé est comparable à une trace de transfert et/ou de contamination. En effet, le laboratoire forensique a employé un plateau en plastique jetable entre le 8 et le 10 octobre 2011 pendant le processus d'extraction de l'ADN du prélèvement issu de la victime. Or, la salive d'Adam Scott se trouvait sur ce plateau suite à un traitement précédent de son échantillon de la muqueuse jugale, mais sans lien aucun avec l'affaire de viol[850].

986 Ainsi, de l'ADN d'Adam Scott a été transféré sur le plateau d'analyse puis sur l'échantillonnage reçu dans le cadre de l'affaire du viol.

987 Fort de constat, Andrew Rennison a été particulièrement choqué de constater que l'usage des plateaux en plastique jetables n'était pas conforme dans ce laboratoire accrédité dès lors qu'ils n'étaient pas jetés systématiquement pouvant causer des identifications erronées[851].

---

[847] RENNISON, p. 1 ss.

[848] RENNISON, p. 10.

[849] RENNISON, p. 1 et p. 8-9.

[850] RENNISON, p. 11-12

[851] RENNISON, p. 1 et p. 5-7.

988 Au vu de ce qui précède, le transfert d'ADN et/ou sa contamination sont des facteurs importants à prendre en considération lors du processus décisionnel en Justice. En effet, malgré l'accréditation des laboratoires et la procédure d'analyse stricte, des erreurs causées par des négligences humaines interviennent. Ces erreurs ont des conséquences fortement dommageables dès lors qu'elles impliquent l'identification d'un suspect, voire d'un coupable, qui n'en est pas un.

989 Pour toutes ces raisons, il est impératif que le juge, lors de l'appréciation de la preuve, effectue un travail minutieux et précis afin de s'assurer de la valeur probatoire de l'analyse ADN apportée au procès.

b) Le mélange et la dégradation

990 Le mélange d'ADN est une trace génétique comprenant deux ou plusieurs ADN. Ce mélange peut avoir lieu avant, pendant ou après la commission de l'acte délictuel, mais précède toujours le prélèvement. Lors de l'analyse génétique, il peut être délicat d'attribuer un allèle à un profil plutôt qu'à un autre. Conséquemment, le résultat identificatoire est complexe, la probabilité est plus incertaine et l'information donnée par l'expert perd de sa force probante.

991 En outre, la bonne résistance de la molécule à l'assaut du temps n'est pas suffisante pour reconnaître un échantillon comme viable. Une bonne comparaison ne peut pas fournir un résultat correct si les échantillons sont dégradés ou conservés dans de mauvaises conditions[852].

992 Une fois à l'extérieur du corps humain, l'ADN n'est plus aussi stable. L'humidité, la chaleur et la lumière sont les trois causes principales détériorant l'ADN indicial ou prélevé.

993 L'eau comprise dans l'humidité est un ingrédient nécessaire pour rompre les liaisons entre nucléotides, ce qui implique un découpage en fragments trop courts de l'ADN qui rend impossible l'amplification. Ce même élément accentue la croissance des bactéries et champignons et actionne les enzymes de dégradation. La chaleur et la lumière jouent également un rôle quant à la dégradation en accélérant les réactions/transformations chimiques.

994 Qu'il s'agisse du matériel génétique non-prélevé ou prélevé mais stocké dans des conditions peu adéquates, les conséquences de la dégradation sont similaires. En cas de dégradation de

[852] ANCEL, p. 164; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 224-225.

moindre importance, il est possible d'établir un profil d'ADN partiel qui rend l'identification possible, mais avec une fiabilité plus faible[853]. En cas d'exposition importante à un ou l'autre des facteurs de dégradation, il se peut que l'analyse ne puisse simplement pas être effectuée. Cette deuxième conséquence limite les chances d'identifier un suspect, extensivement un accusé, voire un coupable, mais sans accusé il n'y a pas de procès et par conséquent les risques de voir l'analyse ADN acceptée sans débat sont inexistants. En revanche, l'établissement d'un profil partiel à son influence sur l'action en justice, il faut impérativement qu'il soit présenté comme tel et que l'expert explique les conséquences de la dégradation pour que le juge puisse apprécier correctement la viabilité de la preuve identificatoire par l'ADN.

c) La contamination

995 De la découverte de la scène de crime jusqu'à l'analyse, l'ADN est manipulé par divers organes. Malgré l'accréditation du laboratoire, le professionnalisme des experts et de la police scientifique, le proverbe "l'erreur est humaine" implique l'existence de risques de contamination. Par ce dernier terme, nous entendons tout événement accidentel/évitable introduisant dans l'échantillon un ADN le polluant[854]. Cette contamination peut provenir de l'environnement entourant les indices, de l'ADN des personnes présentes sur la scène de crime, suite à un éternuement ou des postillons, voire du matériel de prélèvement.

996 A ce sujet, diverses affaires ont marqué l'exploitation de l'analyse ADN comme moyen probatoire. Nous traiterons ici de deux affaires primordiales: le fantôme d'Heilbronn ainsi que l'affaire Farah Abdulkadir Jama et nous limiterons à rappeler l'affaire Adam Scott[855].

997 L'affaire dite du "fantôme d'Heilbronn" est un parfait exemple des risques de contamination et de leurs conséquences. Depuis 1993, suite aux investigations effectuées après le meurtre d'un sexagénaire, une trace ADN est recensée comme appartenant à une femme sans que l'identification ne donne un résultat positif. Durant une dizaine d'année, le personnage du "fantôme d'Heilbronn" n'a jamais réitéré d'infractions jusqu'au 25 avril 2007 où, à 500 km du premier meurtre, une jeune policière de 22 ans est assassinée. Dès cette date, la découverte du même ADN devient fréquent tant sur des scènes de meurtre que sur les lieux d'infractions diverses.

---

[853] MANAOUIL, WERBROUCK, TRAULLE, CORDIER, GIGNON, JARDE, p. 22; VUILLE, Thèse, p. 127.

[854] BUSCH, p. 638; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 241; KLUMPE, p. 27; VUILLE, Thèse, p. 129.

[855] Supra Partie II, Chapitre 2, II, C, 1, b, ii, a), n° 981-987.

998 Pendant plusieurs années, les polices allemande et autrichienne mobilisent près de deux cent enquêteurs sans obtenir de résultat, mais ils constatent des incohérences quant à la nature des crimes, au profil des victimes et aux distances parcourues – en Allemagne, en Autriche et même en France – par le "fantôme d'Heilbronn".

999 En mars 2009, l'enquête aboutit enfin, le "fantôme d'Heilbronn" est une femme innocente de 41 ans travaillant dans une entreprise médicale fournissant les bâtonnets d'analyse à la police scientifique.

1000 En 2011, en Suisse, une affaire similaire au "fantôme d'Heilbronn" a été découverte. Un ADN féminin a été retrouvé sur diverses scènes de crime qui ne semblaient pas être liés entre eux. Il s'est avéré que l'ADN retrouvé était celui d'une femme employée par l'entreprise fabriquant le matériel de prélèvement[856].

1001 Ces affaires démontrent que les problèmes de contamination doivent être considérés avec particulièrement d'attention. Ce d'autant qu'avec l'amplification PCR, il suffit de peu d'ADN intrus pour être détecté et fausser les résultats. Certaines mesures peuvent limiter les risques d'ADN contaminé comme l'élaboration d'une méthodologie de prélèvement, la formation de terrain des enquêteurs, la protection rapide de la scène de crime, l'utilisation d'éléments de protection (masque, gant, blouse, etc.) et d'instruments (pince, scalpel, emballage unitaire, scellé apposé, etc.) à usage unique[857]. Néanmoins, comme le démontre l'affaire du "fantôme d'Heilbronn", l'élimination complète des risques de contamination est impossible.

1002 L'affaire Jamal est un autre exemple des problématiques liées à la contamination[858]. Dans cet affaire, l'erreur n'est pas lié à l'identification du suspect, mais au mécanisme d'identification.

1003 Farah Abdulkadir Jamal a été reconnu coupable, en juillet 2008, par la Cour du comté de Melbourne de viol et détenu pendant 15 mois avant que sa déclaration de culpabilité soit annulée et un acquittement soit prononcé par la Cour d'appel[859]. La condamnation de Farah Abdulkadir Jamal reposait exclusivement sur le fait que son ADN, avec une probabilité exceptionnellement élevée, avait été trouvé sur un écouvillon issu des analyses effectuées sur des femmes qui prétendaient avoir été violées alors qu'elles étaient inconscientes[860].

---

[856] SEILER Martin, *La Suisse a aussi chassé un fantôme, Matériel de prélèvement ADN contaminé*, Zurich 2011.

[857] VINCENT, p. 48 ss.

[858] Information disponible sur le site internet du Département de la justice de la Nouvelle Zélande: http://www.publicdefenders.lawlink.nsw.gov.au/ [consulté le 08.05.2016]; VINCENT, p. 1 ss.

[859] VINCENT, p. 13.

[860] VINCENT, p. 9.

1004 Aucun autre élément de l'enquête ne permettait de relier le coupable à la scène de crime et/ou à la victime. Malgré ceci, son alibi fût simplement rejeté.

1005 Une enquête subséquente diligenté par l'ex-juge Frank H. R. Vincent, a révélé que l'ADN de Farah Abdulkadir Jamal avait été contaminé lors de la collecte défectueuse des échantillons en salle d'examen de l'Hôpital[861]. En effet, l'ex-juge a constaté que l'écouvillon et la lame avaient été recueillis dans la même unité et par le même médecin que celui chargé des échantillons médicolégaux prélevés sur une femme qui avait eu des rapports sexuels avec Farah Abdulkadir Jama[862].

1006 Frank H. R. Vincent a conclu qu'il existait un risque assez élevé qu'une quantité microscopique du prélèvement contenant des données génétiques de Farah Abdulkadir Jama ait été transférée de la première femme à un écouvillon et une lame obtenus lors de l'examen d'une seconde femme, compte tenu de la présence et de l'analyse des échantillons des deux femmes dans un milieu où une telle erreur peut facilement se produire[863].

1007 Sans créer une paranoïa qui risquerait de paralyser le travail des laboratoires ou le recours à l'identification génétique, la contamination peut être à l'origine d'une mauvaise interprétation de la concordance des profils d'ADN[864] – fausse inculpation ou fausse exclusion – surtout si elle n'est pas détectée. Il est nécessaire pour le juge du fond d'analyser l'influence des risques sur la valeur probatoire d'une preuve ADN et non pas simplement se positionner en reconnaissant une force scientifique à ce mode identificatoire.

d) Les autres facteurs

1008 Outre la contamination, d'autres sources peuvent amener à un résultat identificatoire erroné: interversion des échantillons – grand classique des erreurs humaines –, erreur de lecture du profil d'ADN, erreur relative à l'utilisation inadéquate de traces non pertinentes – notamment, les traces de transfert –, problème d'interférence – notamment interférence des divers réactifs pouvant être utilisés pour effectuer le prélèvement selon la surface exploitée – pouvant diminuer ou maximiser les chances des prélèvements du matériel biologique et de son analyse, ou encore erreur d'interprétation des résultats[865].

---

[861] VINCENT, p. 10 et 24.

[862] VINCENT, p. 10.

[863] VINCENT, p. 24.

[864] ANCEL, p. 153; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 241-242; VINCENT, p. 9.

[865] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 248-253; KLUMPE, p. 28-33; MALAUZAT, p. 80.

1009 Le problème des "faux positifs" ne doit également pas être négligé. Un "faux positif" est un résultat identificatoire erroné. Les causes de l'erreur peuvent être diverses: mauvaise interprétation des résultats, mauvaise manipulation lors de la récolte de la trace génétique, etc. Beaucoup de scientifiques s'accordent à reconnaître que les erreurs ne sont pas inexistantes. En revanche, l'ampleur de la fréquence des "faux positifs" n'a pour l'heure fait l'objet d'aucune étude. Tant qu'une erreur est possible et que les risques de faux positifs sont réels, il serait préférable d'affirmer que "la probabilité apparente de correspondance entre deux profils est de X%" plutôt que d'être catégorique sur le résultat probabiliste.

1010 D'un point de vue scientifique, il est au surplus délicat de déterminer quand une trace biologique a été déposée sur les lieux d'une infraction. Dès lors que le dépôt du matériel génétique est fréquent, il se peut que la trace précède ou succède à la commission de l'infraction sans y être liée. Ainsi, pour regrouper une trace indiciale avec une scène de crime et, plus précisément, avec la perpétration de l'infraction, le seul profilage ADN n'est pas suffisant. Généralement, le moment du dépôt est déterminé à l'aide d'autres éléments extérieurs aux sciences forensiques.

1011 L'ADN a encore une image très favorable devant les tribunaux. Il est certain que ce mode probatoire a des atouts majeurs. Toutefois, conséquemment à notre analyse, il est démontré que l'analyse génétique à des fins identificatoires n'est pas infaillible. C'est pourquoi il est préconisé que les juristes effectuent une réflexion rationnelle en considérant les possibles détériorations et contaminations des échantillons ainsi que les risques d'erreur ou d'inférences, et en reconnaissant une force probante moindre à l'identification compromise par rapport à celle effectuée dans les conditions adéquates.

iii. Les limites des probabilités et le manque de formation des juristes

1012 Sans débat, l'appréciation de la preuve est largement limitée forçant les hommes de loi à porter une grande confiance aux résultats et à l'interprétation de l'expert, ce d'autant qu'ils ne peuvent s'écarter du rapport d'expertise qu'en motivant leur doute[866]. Cependant, pour discuter, interpréter, argumenter, voire rejeter les conclusions de l'expert, les juristes doivent pouvoir bénéficier d'une formation suffisante et d'une collaboration plus étroite avec les scientifiques pour leur permettre d'appréhender au mieux la preuve matérielle apportée au procès.

[866] ATF 118 Ia 144, 146-147. Supra Partie II, Chapitre 1, III, C, 1, n° 498-499.

1013 Ces constats nous forcent à nous interroger sur l'appréciation faite des expertises, les limites des résultats exposés en termes de probabilité et le manque de formation des juristes dans les domaines des probabilités et de la génétique pour cerner adéquatement l'identification génétique.

a) Les limites des probabilités

1014 Beaucoup voient dans l'analyse ADN une preuve immédiate et infaillible d'identifier l'auteur d'un crime. Cette approche conduit à se focaliser sur le résultat sans prendre en considération le degré de certitude[867].

1015 L'usage des probabilités permet d'éviter la vision dichotomique – coupable ou non coupable – de la preuve par l'ADN. En théorie, le fait de calculer la valeur probante à l'aide des probabilités et de justifier les éléments de calculs concrétisent la nécessité d'examiner la preuve génétique avec vigilance, en gardant un esprit critique[868]. La soumission du résultat en terme mathématique contribue à nier qu'une identification puisse être absolue alors que seule une partie de l'ADN est analysée et que les coïncidences fortuites ou profils partiels existent.

1016 Dans la pratique, le maintien de l'esprit critique permettant d'appréhender correctement l'identification par l'ADN n'est possible qu'en considérant l'entièreté du processus identificatoire et en comprenant les probabilités énoncées par l'expert. Sans connaissances suffisantes dans le domaine de la génétique et des mathématiques, il est difficile, voire impossible, de saisir le cheminement effectué pour obtenir un résultat identificatoire et le résultat lui-même.

1017 La complexité des mathématiques employées pour déterminer le résultat de l'identification ne doit normalement pas inciter les magistrats à s'appuyer les yeux fermés sur le rapport d'expertise. Néanmoins, faute de compréhension complète du langage mathématique par le magistrat, l'approche statistique pose d'importants problèmes de communication entre l'expert et les juristes impliquant une occultation de la valeur probatoire[869].

---

[867] LINDLEY, p. 85-87; VUILLE, Thèse, p. 165.

[868] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 303-304; KLUMPE, p. 265-266.

[869] ANTOGNINI, p. 13; CHAMPOD, TARONI, RPS 1993, p. 234; ROHMER, Thèse, p. 126; VUILLE, TARONI, forumpoenale, p. 368.

1018 Pour satisfaire pleinement aux règles régissant la preuve pénale et son administration, il est nécessaire que les scientifiques et les juristes communiquent afin que ces derniers comprennent et interprètent les probabilités fournies, les risques de coïncidences fortuites ou d'erreurs ainsi que leurs conséquences, etc. Cette nécessité de compréhension et d'interprétation vise à déterminer précisément si la preuve apportée est pertinente ou non, voire à permettre au juge de s'écarter de l'avis rendu par le spécialiste scientifique en motivant sa décision. En somme, les juristes doivent concevoir que l'apport de l'expert se résume à déterminer le *Likelihood Ratio* et non pas d'apprécier la culpabilité de l'accusé[870].

1019 En outre, les fréquences d'apparition et le résultat probabiliste peut mener à des risques de confusion. La preuve identificatoire par l'ADN se construit sur une approche classique de l'investigation policière, sa fonction est uniquement de compléter l'enquête et non pas de la remplacer[871]. Elle ne fournit qu'un résultat concernant l'origine de la trace biologique indiciale, mais ne démontre pas la culpabilité ou l'innocence d'un individu. Pour éviter les malentendus concernant l'identification par l'ADN, l'expert doit exprimer clairement ce que la nature scientifique de la preuve démontre et les magistrats doivent pouvoir comprendre par eux-mêmes les probabilités.

b) Le manque de formation des juristes

1020 Aux prises avec une décision difficile, qu'ils appréhendent mal, les magistrats fondent leur décision sur l'autorité formelle d'une personne. En d'autres termes, la décision complexe qui ressort d'une étude scientifique ou technique revient à avoir confiance en l'expert. Dénué de toutes connaissances spécifiques en matière de génétique, les juristes ne peuvent discuter le réel bien-fondé de la preuve qu'on leur expose.

1021 Cependant, les magistrats doivent garder à l'esprit que l'ADN n'est qu'un élément venant confirmer ou infirmer les directions de l'enquête et reste soumis à leur libre appréciation. Pour accomplir adéquatement leur mission, les débats lors des procès pénaux sur la preuve identificatoire par l'ADN sont essentiels. Les juristes ont conscience que certaines questions se posent et que la méthode identificatoire ne fournit pas une certitude. Cependant, ils comprennent mal les probabilités qui leur sont exposées et imaginent à peine qu'une trace puisse avoir été déposée bien avant la commission de l'infraction.

[870] CHAMPOD, TARONI, RPS 1993, p. 228.

[871] ANCEL, p. 202; TARONI, preuve ADN, p. 288-289.

1022 Par conséquent, pour évaluer la preuve correctement, les juristes doivent recevoir une formation adéquate et collaborer de manière accrue avec les experts scientifiques – explication de l'approche probabiliste aux juristes, traduction des données chiffrées, etc. –, sans quoi aucune évaluation de la force probante ne peut être correctement effectuée. A notre avis et en accord avec la doctrine[872], il est essentiel que les juristes se familiarisent avec la théorie mathématique de la preuve génétique et qu'ils forcent les experts à expliciter les étapes de leur raisonnement à l'aide de questions spécifiques.

iv. Le renversement du fardeau de la preuve

1023 Dans un arrêt du 7 octobre 2011[873], le Tribunal fédéral a rejeté le recours d'un condamné qui s'est plaint d'une appréciation arbitraire des faits quant à l'absence d'ADN sur le corps de la victime, plus précisément dans ses parties génitales. Le recourant allègue qu'il n'a pas violé la victime, mais il reconnaît avoir introduit son doigt dans son vagin et son anus.

1024 Le Tribunal fédéral rejette le recours, notamment, en considérant que le recourant n'apportait "aucun élément concret, scientifique en particulier, susceptible de démontrer que la pénétration digitale qu'il allègue laisserait nécessairement moins de traces ADN que l'intromission d'un pénis". Cette argumentation revient à renverser le fardeau de la preuve[874].

1025 En droit pénal, la présomption d'innocence est l'un des principes fondamentaux de la procédure. Si le Tribunal fédéral regrette de ne pas pouvoir bénéficier des analyses ADN dans le cas d'espèce, cela ne l'autorise pas à demander au condamné de prouver qu'il n'a pas commis un acte.

1026 En outre, à notre avis, le Tribunal fédéral est dans l'erreur scientifiquement parlant. S'il est viable de demander à quelqu'un de prouver que son ADN n'est pas le sien ou, tout du moins, qu'il ne correspond pas à l'ADN trouvé sur la victime, il est en revanche impossible de démontrer par une trace génétique quels sont les événements qui se sont déroulés. Ainsi, la découverte d'une trace ADN ne dit rien des activités ayant occasionné son dépôt[875].

---

[872] ANTOGNINI, p. 11 et 13; CHAMPOD, TARONI, RPS 1993, p. 235; CHAMPOD, TARONI, RPS 1994, p. 213; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 303ss; JACKSON, p. 85; MANGIN, TARONI, p. 510; ROHMER, Thèse, p. 127; TARONI, preuve ADN, p. 276 et 290; TARONI, AITKEN, p. 292.

[873] TF 6B_150/2011 du 7 octobre 2011.

[874] VUILLE, forumpoenale, p. 248.

[875] VUILLE, forumpoenale, p. 249.

1027 Alors qu'actuellement la science ne permet pas d'évaluer les activités pouvant mener au dépôt d'une trace ADN avec une force probante suffisante, nous pouvons constater – une nouvelle fois – que le manque de connaissance des juristes peut engendrer des demandes déraisonnables de la part des juges. Il ne faut pas perdre de vue que les indices scientifiques ne peuvent pas tout prouver.

1028 Relevons que le Tribunal fédéral s'est également appuyé sur l'avis d'une experte pour rejeter le recours. A ce sujet, il est intéressant de noter que la doctoresse n'a pas évalué les hypothèses pouvant expliquer l'absence d'ADN dans les organes génitaux de la victime. Elle s'est bornée à affirmer qu'il est possible de ne trouver aucun spermatozoïde lors d'une pénétration non protégée sans éjaculation. Cette affirmation sans qualification de son degré de probabilité n'aurait pas dû être déclarée comme une preuve pertinente (art. 139 al. 2 CPP).

1029 Cet arrêt permet d'étayer le fait que les juristes ont théoriquement le pouvoir d'apprécier les expertises, mais, à défaut de connaissances scientifiques suffisantes, il laisse bien souvent la décision entre les mains des experts.

2. L'utilisation du système CODIS et ses limites

1030 Le prélèvement, l'échantillonnage, l'établissement du profil sont des étapes clés, mais insuffisantes pour révéler l'importance de l'ADN dans le monde judiciaire. La comparaison des profils et la réalisation d'un hit sont l'essence même de ce moyen de contrainte, puisqu'elles permettent l'identification du profil génétique analysé, voire l'élucidation d'un crime (art. 255 al. 1 et 256 CPP) ou d'un délit (art. 255 al. 1 CPP).

1031 Le pouvoir identificatoire de l'ADN a influé sur le travail de la police et du système judiciaire avec pour incidence la création d'une base de données des profils génétiques[876]. En l'absence d'un fichier automatisé comparatif, le profil génétique ne fournit pas l'entier de son pouvoir identificatoire. La mise en place du système CODIS a pallié ce manque.

1032 L'informatique est un outil précieux d'entraide pour confronter une multitude de données et facilite la conservation ainsi que la consultation des fiches automatisées. En contrepartie, l'automatisation des données génétiques crée un risque d'atteinte à la vie privée, à la liberté personnelle et peut mener faussement à la conclusion d'une enquête, voire d'un procès. La présente partie tente de mettre en exergue les points positifs de la base de données CODIS, tout en pointant les désavantages à prendre en considération ou à surveiller.

[876] ANCEL, p. 206; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 421; MOUSTIERS, p. 167.

a. L'efficacité et les avantages du système automatisé CODIS

i. Un outil d'enquête et d'entraide à la poursuite pénale

1033 Le processus de fichage débute par l'interpellation d'une personne, le prélèvement de son matériel génétique et l'analyse génétique subséquente[877]. Le profil d'ADN obtenu est intégré provisoirement à la base de données CODIS pour être confronté aux profils stockés et éventuellement à la trace indiciale d'origine inconnue. L'intégration de la fiche informatisée ne devient définitive qu'en cas de condamnation.

1034 L'efficience du fichier CODIS est proportionnelle au nombre de fiches incorporées, plus le nombre de profils enregistrés est important plus les chances d'identification augmentent. La disponibilité des fiches d'ADN a pour conséquence un déplacement de l'analyse génétique en début d'enquête pour cibler un potentiel suspect[878]. Au début de l'utilisation du matériel génétique comme moyen identificatoire, le prélèvement et l'analyse de l'ADN n'avaient lieu qu'en fin d'enquête pour conforter les soupçons sur le suspect. Aujourd'hui, grâce au fichier informatisé qui facilite les comparaisons, le profil d'ADN est utilisé pour désigner un suspect de manière efficace et relativement fiable[879].

1035 Au-delà de la facilité d'obtenir une information, la comparaison informatisée s'effectue en peu de temps permettant l'accélération des procédures.

1036 La rapidité de comparaison et l'augmentation du nombre de profils stockés dans CODIS n'est pas sans influence sur l'économie du procès. Premièrement, le temps gagné à éviter des interrogatoires fastidieux lorsque l'individu nie tout lien avec la victime, le lieu de l'infraction ou un objet s'y référant permet au corps de police de se focaliser sur une autre affaire ou une autre tâche.

1037 Deuxièmement, une seule analyse génétique peut servir à établir un lien entre plusieurs affaires – même séparées dans le temps ou dans l'espace – impliquant une dispense pour les enquêteurs d'investigations classiques[880]. Grâce à la base de données CODIS, il suffit qu'un malfaiteur soit arrêté et fasse l'objet d'un prélèvement pour réaliser qu'il est à la source d'une

[877] Supra Partie II, Chapitre 2, II, A, 4, n° 827 ss.

[878] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 421; CR-CPP-ROHMER, art. 255 N 5.

[879] COQUOZ, p. 173; COQUOZ, COMTE, HALL, HICKS, TARONI, p. 421; GIROD, MARGOT, RIBAUX, WALSH, p. 135.

[880] ANCEL, p. 144; GIROD, RIBAUX, MARGOT, WALSH, p. 136.

série de traces biologiques déjà découvertes. Dans ces circonstances, la fonction identificatrice de l'ADN est pleinement remplie et conforte les milieux policiers dans leurs démarches[881].

1038 Enfin, la comparaison individu/individu permet de déceler les substitutions éventuelles d'identités.

1039 Le taux d'élucidation de crimes ou délits, extensivement le nombre de poursuites et de condamnations, ont sensiblement augmenté grâce à CODIS[882]. En augmentant les chances d'identification des criminels et en assurant par là-même une meilleure sécurité publique, la base de données CODIS a également un effet dissuasif. Les possibilités accrues de hit grâce au nombre de fiches enregistrées s'accompagnent d'une crainte des auteurs d'actes délictuels de se voir systématiquement identifier entraînant une baisse de la commission des crimes et délits.

ii. L'atteinte aux libertés fondamentales partiellement amoindrie

1040 Nous avons précédemment constaté que le prélèvement du matériel génétique et l'intégration du profil d'ADN atteignaient de manière plus ou moins légère à certaines libertés fondamentales[883]. Nonobstant ces atteintes, il est également possible d'affirmer que la création de la base de données CODIS et son utilisation croissante favorisent dans certaines circonstances une diminution des atteintes aux droits fondamentaux.

a) La limitation possible des enquêtes de grandes envergures

1041 La possibilité offerte par CODIS de répertorier un grand nombre de profils d'ADN de criminels permettant d'identifier plus aisément l'auteur à l'origine d'une trace influe sur la nécessité d'effectuer des enquêtes de grandes envergures[884]. Nous avons déjà exposé que le nombre de profils est interdépendant à la réussite de l'analyse de comparaison. Dès lors, l'identification étant plus aisée, l'obtention d'un échantillonnage important peut se révéler désuet.

---

881 GIROD, RIBAUX, MARGOT, WALSH, p. 136.

882 GIROD, MARGOT, RIBAUX, WALSH, p. 145-146; KILLIAS, HAAS, TARONI, MARGOT, p. 305.

883 Supra Partie II, Chapitre 2, II, B, 1, a, n° 845 ss; Infra Partie II, Chapitre 2, II, C, 2, c, n° 1060.

884 KILLIAS, HAAS, TARONI, MARGOT, p. 304.

1042 Prenons un exemple: une trace est découverte sur les lieux d'un crime dont l'accès est sécurisé, la police n'a aucun suspect, leur soupçon se porte uniquement sur les vingt employés de sexe masculin habilités à pénétrer dans ledit lieu; grâce à la base de données, il est possible qu'une comparaison entre la trace et les profils d'ADN s'avère positive. Ainsi, il est non seulement possible de limiter les coûts – économie du matériel de prélèvement et d'analyse d'échantillons –, le temps nécessaire aux experts et surtout les atteintes à la liberté personnelle des individus devant être soumis au prélèvement. En effet, l'identification fournissant possiblement un résultat grâce aux profils déjà répertoriés, il n'est pas nécessaire d'effectuer un frottis de la muqueuse jugale ou un prélèvement sanguin sur toute une série d'individus, prélèvement qui crée une atteinte à la liberté personnelle, plus spécifiquement corporelle, de toutes les personnes concernées.

b) Les avantages de l'anonymisation

1043 Le deuxième amoindrissement d'une atteinte à un droit fondamental est celui découlant de la technique même de stockage.

1044 Grâce à l'informatique, il est possible de répertorier de manière anonyme les profils – et non pas le code génétique dans son entier – permettant l'identification de l'auteur sans prendre connaissance de ses caractéristiques personnelles, outre le sexe, et de lier les données personnelles avec le profil anonymisé qu'en cas de besoin. De ce fait, le système CODIS est moins invasif que le casier judiciaire qui contient les antécédents et les données personnelles de l'intéressé.

1045 Au surplus, le rapprochement des données avec le profil d'ADN ne s'effectuent pas par l'organe d'enquête, mais par un service de la Fedpol ce qui limite fortement l'accès aux données personnelles, extensivement diminue l'atteinte à l'autodétermination informationnelle.

c) La limitation des ingérences à la sphère privée des individus innocents

1046 Les défenseurs de la protection de la sphère privée peuvent saluer la base de données CODIS.

1047 En effet, la première étape d'enquête sert à découvrir un suspect. Si elle est réalisée correctement et à l'aide d'un profilage ADN, il est possible de ne pas soupçonner une

personne clairement innocente limitant les interrogatoires, les questions indiscrètes et la possible mise au pilori d'un innocent par ses proches[885].

b. Les risques liés à l'utilisation et à la croissance de CODIS

i. La négligence des autres éléments de l'enquête

1048 Avec l'aisance que procure l'exploitation de CODIS, le danger de voir les enquêteurs attendre les résultats de l'analyse génétique avant d'entreprendre les démarches d'investigation, voire de limiter leurs efforts pour collecter des informations essentielles en cas de traces non-pertinentes, ne peuvent être écartés[886].

1049 La base de données CODIS ne doit pas mettre en péril la tâche d'investigation et de récolte de preuves essentielles pour créer un faisceau de preuves – en cas de traces pertinentes – ou apporter une autre vision de l'affaire – découverte de traces non-pertinentes[887].

1050 Dans la première situation, certes la récolte d'informations pourrait corroborer les résultats de l'analyse ADN, mais elle pourrait aussi contredire ou apporter d'autres hypothèses du déroulement des faits. C'est pourquoi un résultat identificatoire n'est pas suffisant pour juger l'affaire et les investigations doivent impérativement être réalisées. Rappelons, au surplus, que le facteur temps peut dégrader un certain nombre d'indices ou rendre difficile la poursuite d'un suspect, il n'est dès lors pas possible d'attendre le résultat d'analyse génétique pour mettre en marche toute la phase d'enquête.

1051 Dans la seconde circonstance, l'utilisation des traces non-pertinentes constitue un autre risque qui s'accroît avec la mise en œuvre d'un système automatisé. En effet, la comparaison étant facilitée par l'informatique, bon nombre de traces sont comparées alors même qu'avec un peu de réflexion elles seraient écartées faute de pouvoir ou d'être liées à l'affaire.

1052 Le gain de temps et la facilité d'identifier un individu sont deux arguments favorables pour l'utilisation de l'ADN comme moyen identificatoire par les services d'enquête. La découverte d'une trace étant pratiquement toujours possible, l'analyse subséquente l'est également. Cela ne signifie pas pour autant que l'individu à la source de cette trace ait un lien avec l'infraction constatée.

---

[885] COQUOZ, p. 173-174.

[886] COQUOZ, COMTE, HALL, HICKS, TARONI, p. 431; COQUOZ, p. 174; ROUX, p. 182.

[887] MANAOUIL, WERBROUCK, TRAULLE, CORDIER, GIGNON, JARDE, p. 22; MARGOT, CHAMPOD, p. 246; PADOVA, p. 72.

1053 Ainsi, même si la base de données fournit un résultat positif, celui-ci n'est rien si les magistrats ne l'examinent pas avec un esprit critique. Il faut impérativement que les juristes comprennent que si l'identification est de plus en plus facilitée à mesure que le fichier automatisé s'agrandit et se perfectionne, elle n'en est pas moins incertaine.

ii. La sécurité du fichier informatisé

1054 La popularisation de l'informatique s'est accompagnée du développement du hacking. Sous ce terme se dissimulent les hackers, soit des utilisateurs passionnés d'informatique désirant vérifier la sécurité des réseaux, voler ou modifier des données informatisées, espionner, etc. Quoi de mieux pour se défendre que de détruire la preuve génétique ou de modifier son profil d'ADN pour s'innocenter?

1055 En août 2003, un expert en sécurité informatique s'est infiltré dans le fichier des patients d'un hôpital zurichois[888]. Huit ans plus tard, la société de sécurité informatique "McAfee" a révélé que septante-deux organisations mondiales, notamment le gouvernement américain, l'ONU, le CIO, ont été infiltrées par du cyberespionnage[889]. En 2014, le cyberespionnage "The Mask", ayant pour but de collecter des données sensibles, a infiltré des sites suisses notamment l'administration, et trente autres pays, ce sont alors des représentations diplomatiques, des ambassades, des compagnies pétrolières, gazières et énergétiques ainsi que des laboratoires de recherche qui ont été touchées[890]. En mai 2016, le conseiller fédéral Guy Parmelin annonce qu'en janvier, durant le World Economic Forum, des pirates informatiques se sont attaqués au site internet du Département de la défense et de la société Ruag qui a des liens étroits avec l'armée[891]. Les dommages ne sont pas encore connus. Une enquête diligentée par le Ministère public de la Confédération est en cours.

1056 Ces exemples parmi tant d'autres illustrent la faillibilité des systèmes informatiques encore aujourd'hui.

1057 En outre, la sécurité physique du fichier doit également être assurée pour éviter toutes destructions ou altérations des données, par exemple par le feu.

---

[888] Le Temps, *Les informations médicales à la merci des hackers*, article du 11 août 2003.

[889] Le Temps, *La menace chinoise*, article du 5 août 2011.

[890] ICT journal, *L'attaque de cyberespionnage "The Mask" a touché la Suisse*, article du 11 février 2014.

[891] Le Temps, *Le Département de la défense a été attaqué par des hackers*, article du 4 mai 2016; Tages Anzeiger, *Cyberangriffe aus Moskau*, article du 4 mai 2016.

1058 Les risques de voir le fichier détruit matériellement ou techniquement ne sont pas inexistants. Dès lors, pour lutter le plus efficacement possible contre le piratage et éviter la destruction d'informations, il est important de sécuriser le réseau de transmission des données.

1059 En Suisse, concernant le fichier CODIS, les conditions sécuritaires sont pleinement remplies. Cependant, une attaque liée à une faille inconnue est toujours possible pouvant impliquer une perte d'informations ou une atteinte aux droits de la personnalité avec l'accès aux données personnelles. Les magistrats doivent donc prendre acte que, malgré la reconnaissance de l'identification par l'ADN, un système de base de données est faillible et qu'il n'est pas possible de s'y fier les yeux fermés. Ils devront notamment s'assurer qu'aucun accès illicite aux fichiers n'a eu lieu et qu'aucune modification injustifiée n'a été réalisée.

c. Le profilage ADN automatisé à la lumière de la liberté personnelle et de la sphère privée

1060 Comme nous l'avons préalablement indiqué, le prélèvement, l'analyse et la comparaison des profils d'ADN peuvent porter atteinte aux droits fondamentaux[892]. Nous nous focaliserons dans la présente partie à la possible violation de la présomption d'innocence ainsi qu'à la mise en péril de la sphère privée et du droit à l'autodétermination informationnelle liées à l'intégration et la conservation des profils génétiques dans CODIS.

i. La présomption d'innocence

1061 La première critique généralement formulée contre le système CODIS est la violation de la présomption d'innocence[893]. D'après ce principe, aucune mesure de contrainte ne peut être ordonnée sans qu'il existe des soupçons suffisants.

1062 Ainsi, si un profil est conservé et qu'une recherche est effectuée à l'aide du fichier CODIS alors même qu'aucun soupçon n'existe, le comportement de l'autorité pénale viole la présomption d'innocence. En revanche, ce principe fondamental de la procédure pénale n'interdit pas qu'une source d'informations provenant d'affaires antérieures puisse servir pour en déduire des soupçons.

---

[892] Supra Partie II, Chapitre 2, II, B, 1, a, n° 845 ss.

[893] KILLIAS, HAAS, TARONI, MARGOT, p. 307; ROUX, p. 185-186.

1063 Par conséquent, l'utilisation notamment des fichiers de profil génétique lors d'enquête ne viole en aucun cas la présomption d'innocence. La critique formulée par certains scientifiques ou juristes doit donc être réfutée.

ii. Le droit à l'autodétermination informationnelle et la sphère privée

1064 La seconde critique concerne le droit à l'autodétermination informationnelle et la sphère privée[894].

1065 En accord avec l'arrêt *Amann* c. *Suisse*[895], le Tribunal fédéral reconnaît que toute mémorisation par une autorité publique des données relative à la vie privée atteint à l'art. 8 § 1 CEDH – corrélativement à l'art. 13 al. 1 Cst – et que le stockage des profils d'ADN restreint la liberté personnelle[896]. Concernant la gravité de cette atteinte, elle est interdépendante avec le sort réservé aux échantillons ayant servi de base au profilage et au profil lui-même.

1066 Dans le cadre du profilage ADN, seules les parties non-codantes de l'ADN étant analysées, le Tribunal fédéral a estimé que l'atteinte causée correspondait à l'atteinte subie par le prélèvement d'empreinte digitale, soit une atteinte légère[897].

1067 Ainsi, tant que l'évolution scientifique ne permettra pas de fournir des informations personnelles à l'aide de segment non-codant[898], la réglementation limitant l'établissement d'un profil d'ADN sur la base de segment non-codant est suffisante pour éviter une atteinte illicite aux droits fondamentaux.

1068 Quant au sort des échantillons, afin de se limiter à une atteinte légère, ils doivent être détruits rapidement (art. 9 al. 1 et 2 *cum* 10 à 13 Loi sur les profils d'ADN). Cette destruction se justifie par le respect du principe de la nécessité. En effet, ce n'est pas l'échantillon d'ADN, mais le profil qui découle de son analyse qui est utile à l'identification génétique. Dès lors, la conservation d'un échantillon ne pourrait être utile que pour effectuer un nouveau profilage. Néanmoins, d'autres moyens peuvent permettre une nouvelle analyse, notamment un

---

[894] BUSCH, p. 643; DONATSCH, RPS 1991, p. 182; JOSITSCH, Strafprozessrechts, p. 137-138; KLUMPE, p. 143-144 et 152; OBERHOLZER, DNA, p. 331; ROHMER, Banque de données ADN, p. 203; ROHMER, Thèse, p. 78-79; SCHMID, Handbuch, p. 475; VIREDAZ, p. 323.

[895] CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95.

[896] ATF 120 Ia 147, 149-150 = JdT 1996 IV 61, 61; ATF 128 II 259, 267-268 = JdT 2003 I 411, 419-420 = SJ 2002 I 531, 531.

[897] ATF 128 II 259, 269-270 = JdT 2003 I 411, 420-421 = SJ 2002 I 531; DONATSCH, RPS 1991, p. 185.

[898] KNOPPERS, GRIMAUD, CHOQUETTE, LE BRIS, p. 62.

nouveau prélèvement du matériel génétique de la personne incriminée. A noter également que la destruction doit permettre d'éviter une possible analyse subséquente des parties codantes. Si une telle analyse était réalisée, l'atteinte aux libertés personnelles et au droit à l'autodétermination informationnelle serait considérée comme grave et probablement illicite faute d'adéquation, de nécessité et de proportionnalité[899].

1069 En outre, en tant que système informatisé, CODIS présente des risques liés à l'utilisation abusive des données stockées (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 13 al. 2 Cst). Même si les informations sont anonymisées et que les systèmes CODIS et IPAS sont séparés physiquement et structurellement, il est possible de réunir le profil d'ADN avec des données strictement personnelles contenues dans IPAS. Ces risques sont d'autant plus grands que la sécurité informatique n'est pas garantie à 100%[900]. Une atteinte aggravée au droit à l'autodétermination informationnelle n'est donc pas exclue.

iii. La proportionnalité des atteintes aux droits fondamentaux liées à l'utilisation de CODIS

1070 En fonction des données analysées, du temps de conservation et de la méthode de stockage, la gravité de l'atteinte aux droits fondamentaux causée par l'existence de CODIS varie considérablement.

1071 Dans des circonstances optimales – ADN non-codant analysé, échantillons détruits, sécurités informatiques assurées – l'atteinte à la liberté personnelle et à l'autodétermination est légère, mais si une de ces conditions fait défaut une atteinte grave n'est pas exclue.

1072 Partant de ces constations, la restriction des droits fondamentaux doit s'appuyer sur une base légale, être nécessaire et proportionnée (art. 8 § 2 CEDH et 36 Cst). Concernant la première condition, la loi sur les profils d'ADN et son ordonnance constituent des bases légales suffisantes pour règlementer la conservation des échantillons et des profils d'ADN ainsi que le stockage automatisé de ces derniers. La seconde condition ne pose guère plus de problème, la nécessité de poursuite des infractions avec comme point d'orgue la découverte du ou des auteur(s) d'infraction et la prévention générale contre les actes répréhensibles visent un but d'intérêt public[901]. La base de données CODIS remplit entièrement ce but en

[899] ATF 128 II 259, 268 = JdT 2003 I 411, 419-420 = SJ 2002 I 531.

[900] Supra Partie II, Chapitre 2, II, C, 2, b, ii, n° 1054 ss.

[901] ATF 120 Ia 147, 151 = JdT 1996 IV 61; ATF 126 I 7, 13; ATF 128 II 259, 275 = JdT 2003 I 411, 426 = SJ 2002 I 531; DONATSCH, RPS 1991, p. 191; PFPDT, Rapport 2008/2009, p. 46; ROHMER, Thèse, p. 96-97.

permettant l'identification d'un auteur de trace et, conséquemment, une possible instruction pénale contre lui. Un examen des problématiques liées à la proportionnalité s'impose.

1073 La conservation des profils d'ADN sert à poursuivre les auteurs en les identifiant. Il n'est plus à prouver que plus le nombre de profils d'ADN conservés est important, plus les chances de parvenir à une correspondance sont grandes. En conséquence, l'aptitude de la mesure consistant à ne pas effacer immédiatement les profils est admissible pour poursuivre la criminalité. Quant au respect du principe de nécessité, le stockage des données ne pose guère de problème, dès lors que la durée de conservation dépend étroitement de la gravité de l'acte et de la sanction (art. 16 Loi sur les profils d'ADN).

1074 La question de la proportionnalité au sens strict est plus délicate et discutable.

1075 Selon les décisions des Chambres fédérales, la banque de données CODIS n'intègre que les personnes condamnées à des crimes ou délits, mais pas les auteurs de contraventions. A notre sens, nous pourrions et même devrions ajouter le terme "*intentionnels*" aux crimes et délits commis. En effet, les risques de récidive étant logiquement inexistants pour une personne ayant agi par négligence, l'intérêt public ne pourrait pas justifier l'atteinte aux droits personnels de l'individu concerné.

1076 D'ailleurs, l'art. 257 CPP prévoit expressément que seules les personnes déjà condamnées pour un crime ou un délit intentionnel peuvent faire l'objet d'un prélèvement génétique, extensivement d'une conservation de son profil d'ADN, étant relevé que la let. c de cette disposition légale ne prévoit pas clairement ces conditions, mais que la doctrine s'entend à interpréter cette lettre à l'aune des deux précédentes.

1077 En revanche, ni l'art. 255 et 256 CPP, ni la loi sur les profils d'ADN n'explicitent l'intentionnalité pour la conservation des prélèvements de personnes suspectées et subséquemment condamnées.

1078 Dans le strict respect de la proportionnalité, une précision devrait être apportée aux bases légales existantes pour assurer la légalité de la restriction à la sphère privée et au droit à l'autodétermination informationnelle. A noter qu'il ne s'agit pas d'évaluer *a priori* – lors du prélèvement – si l'infraction est commise intentionnellement ou par négligence[902], mais bien de conserver l'intégration du profil d'ADN uniquement en cas de condamnation pour une infraction intentionnelle.

[902] En contradiction avec: ROHMER, Thèse, p. 121.

d. Les recommandations pour l'avenir

1079 L'utilité de la gestion systématique des profils d'ADN de manière automatisée n'est plus à prouver. Si, aujourd'hui, la sphère privée est relativement bien protégée et assurée par la procédure mise en vigueur, l'avenir accompagné de l'évolution des sciences et des techniques peut apporter son lot d'inquiétudes, ce d'autant qu'il est toujours délicat de prévoir comment va évoluer une science et quelles découvertes vont être réalisées.

i. Le décryptage de la partie codante de l'ADN

1080 Actuellement, l'ADN non-codant ne fournit aucune donnée personnelle ou sensible. Cependant, il n'est pas exclu qu'un jour ces segments puissent être décodés et révèlent une information sensible, mais utile à la procédure pénale[903]. D'ailleurs, une équipe de chercheurs italiens a démontré qu'un segment ADN lié à une maladie génétique rare était analysé par la France lors de profilage ADN, ce qui crée une atteinte potentiellement grave aux droits fondamentaux de l'individu[904]. Dans cette hypothèse, la Loi sur les profils d'ADN serait alors insuffisante pour prévenir toute atteinte grave au droit à l'autodétermination informationnelle.

1081 S'il est exact que le législateur ne peut pas prévoir tout ce qui se passera ou pourrait se passer dans un avenir plus ou moins proche, les juristes doivent toutefois réfléchir à certaines problématiques. En particulier, il est de leur devoir de trouver une solution législative adéquate en cas de déchiffrement de la partie codante, notamment en précisant la loi au regard de la gravité de l'atteinte.

1082 Par exemple, à notre avis, en cas de déchiffrement de la partie non-codante ou si, comme il était initialement prévu dans le projet de loi[905], le législateur décide d'autoriser l'analyse des séquences codantes si cela est nécessaire pour élucider un crime, la restriction du droit d'accès à la banque de données et/ou le cercle de personnes à intégrer dans CODIS – par exemple, en autorisant l'accès et l'intégration de profils pour des crimes ou délits exhaustivement listés – est une solution viable pour respecter le principe de proportionnalité.

---

[903] KNOPPERS, GRIMAUD, CHOQUETTE, LE BRIS, p. 62; PITTELOUD, p. 395; ROHMER, Forumpoenale, p. 347; ROHMER, Thèse, p. 352.

[904] ATF 129 I 232, 245-246 = SJ 2003 I 513, 526; ROHMER, forumpoenale, p. 347.

[905] Projet de loi fédérale sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification des personnes inconnues ou disparues, FF 2001 19, 50.

ii. L'intégration de profils d'ADN d'auteurs de contraventions

1083 Nous l'avons dit[906], la base de données CODIS a été conçue pour identifier les sources des traces biologiques avec une augmentation des chances de réussite proportionnelle au nombre de profils d'ADN intégrés. Une autre évolution possible serait de ne pas limiter l'intégration des profils d'ADN aux simples auteurs de crimes ou délits pour lutter plus efficacement contre la criminalité.

1084 L'intégration des auteurs d'infractions de moindre gravité peut se justifier par les études criminalistiques qui démontrent que les malfaiteurs de crimes ou délits avaient préalablement réalisé des infractions dites bagatelles[907]. Cependant, même s'il est démontré qu'un auteur d'infraction commise auparavant puisse réaliser les éléments objectifs et subjectifs d'un crime ou d'un délit important, cela n'est pas suffisant pour déroger aux impératifs légaux de la restriction des droits fondamentaux (art. 8 § 2 CEDH et art. 36 Cst).

1085 Alors que l'adéquation de la mesure est démontrée par les études criminalistiques et que la nécessité ne pose pas de problème majeur – le recours aux analyses et comparaisons ADN se limite au cas où il est essentiel à la poursuite pénale –, la question de la proportionnalité de la mesure proposée est plus discutable. D'un côté, nous avons l'intérêt public à la lutte contre la criminalité dont l'efficience serait plus importante avec une base de données plus grande, et de l'autre l'autodétermination informationnelle et la sphère privée de l'auteur d'une infraction bagatelle.

1086 En tant que donnée anonymisée, le profil d'ADN sans regroupement avec le fichier IPAS n'atteint que faiblement aux libertés personnelles. En revanche, le regroupement de ces données – qui ne se justifierait pas toujours – fournit des informations sensibles sur l'auteur d'une infraction bagatelle.

1087 C'est pourquoi, s'il est décidé d'intégrer également les profils d'auteur de contravention, la restriction d'accès – en l'autorisant que pour élucider des infractions d'une certaine gravité – respecterait la proportionnalité. L'utilité de la banque de données CODIS ne serait pas réduite, pour autant que l'enregistrement en amont soit large, et l'utilisation abusive de l'IPAS en lien avec une fiche d'ADN pour élucider des infractions de faible importance serait évitée.

---

[906] Supra Partie II, Chapitre 2, II, B, 1, b, ii, n° 886 ss; Supra Partie II, Chapitre 2, C, 2, a, n° 1033 ss.

[907] GIROD, MARGOT, RIBAUX, WALSH, p. 133; KILLIAS, HAAS, TARONI, MARGOT, p. 298-304; SCHMID, Praxiskommentar, art. 255-259 N 4 ss.

D. La synthèse des débats et conclusion

1088 Indiscutablement, la génétique est un mode probatoire essentiel à la procédure pénale. Les bénéfices et l'apport de l'ADN en tant que moyen identificatoire n'est pas à remettre en question. Avec leur puissance d'identification et leur fiabilité, les analyses ADN participent à l'intégration des sciences dans la procédure pénale et à l'élucidation des infractions. En revanche, il est nécessaire de faire preuve de retenue lors de l'administration et l'appréciation de la preuve génétique.

1089 La gestion systématique des liens ADN doit s'inscrire dans une approche globale de l'élucidation de l'infraction concernée, soit dans un faisceau de preuves. Ceci permet de considérer l'identification, plus précisément la présomption qui en faite, grâce au matériel biologique comme une étape élémentaire du renseignement criminel sans lui donner une portée plus large que ce qu'elle démontre.

1090 En d'autres termes, l'intégration de la preuve ADN dans sa considération pure d'indice matériel évite que l'identification ne soit considérée comme une preuve de culpabilité ou d'innocence, dans la mesure où elle n'explique pas comment la trace s'est trouvée sur les lieux de l'infraction, mais uniquement quel est le rapport de vraisemblance que le suspect soit à la source du matériel biologique détecté.

1091 Pour permettre l'utilisation cohérente et judicieuse de la preuve génétique, l'approche probabiliste et la nature scientifique du mode probatoire forcent à instruire les juristes en conséquence. La formation adéquate, initiale et continue des juristes vise une meilleure coordination des services liés au processus identificatoire par l'ADN (juristes, analystes, enquêteurs, etc.). En effet, sans compréhension et discussion entre les différents acteurs, il est difficile d'évaluer correctement la valeur de la preuve apportée au procès et les risques d'incertitude pouvant exister.

1092 Actuellement, faute de connaissances adéquates, la libre appréciation de la preuve génétique est souvent inexistante à l'égal des débats sur la qualité de l'identification par l'ADN. Il ressort que, bien souvent, la valeur probatoire est reconnue uniquement en s'appuyant sur la valeur scientifique. Par manque de compréhension et de connaissances, les juristes ne peuvent pas motiver l'exclusion du rapport d'expertise, débattre sur la preuve génétique ou évaluer la force de conviction impliquant que la décision finale relative à l'identification est souvent calquée sur les conclusions de l'expert.

1093 Ce constat nous mène à conclure que le déroulement actuel de l'administration de la preuve génétique est insatisfaisant au regard des principes de procédure pénale, spécifiquement du droit de la preuve. Ainsi, la prise de certaines mesures est essentielle pour éviter que l'apparente perfection technique des outils scientifiques prenne une place centrale dans la décision de culpabilité.

CHAPITRE 3: LES PREUVES FONDÉES SUR LES TECHNIQUES

1094 Offrant des capacités significatives en justice criminelle, les nouvelles technologies se sont naturellement intégrées au travail des enquêteurs pour lutter contre la nouvelle criminalité, localiser les criminels, les identifier et collecter toutes les informations utiles à l'élucidation d'un acte criminel[908].

1095 Les techniques existantes pouvant servir à la justice étant nombreuses et variées, nous avons choisi d'analyser celles qui sont utilisées le plus couramment et qui paraissent fournir une preuve *a priori* suffisamment accablante de la culpabilité du contrevenant ou de son innocence. Les interceptions des télécommunications et la surveillance visuelle sont les techniques dites de surveillance (I.) les plus notoirement connues. Elles sont considérées comme des modes d'investigation efficaces pour intercepter les criminels, le contenu de leurs communications et/ou leurs faits et gestes. A ces techniques de surveillance viennent s'ajouter celles de localisation (II.) – utilisation du système GPS ou de téléphonie mobile – qui sont usitées pour replacer dans l'espace et dans le temps le criminel sur les lieux de l'infraction. En outre, l'utilisation de l'informatique (III.) tant par la population que par les enquêteurs est un moyen adéquat pour servir la justice. Dans le premier des cas, les disques durs, historiques internet ou autres données informatiques regorgent d'informations pouvant être utilisées comme moyens probatoires. Dans le second cas, l'informatique aide à l'enquête en regroupant facilement les informations collectées sur l'affaire ou le suspect et en les comparant pour obtenir un résultat identificatoire ou pour établir le déroulement des événements.

1096 De prime abord, la classification des techniques en diverses catégories – de surveillance, de localisation ou informatique – peut paraître arbitraire, puisque la surveillance des télécommunications, la localisation par GPS et la vidéosurveillance emploient également des systèmes informatisés. Il nous faut donc préciser que le découpage réalisé s'appuie sur la finalité ou le but premier de la technique et non pas sur les systèmes accessoires devant être employés.

1097 Corrélativement aux développements concernant les sciences, la présente partie se compose de l'exposé des aspects techniques et juridiques de divers moyens technologiques dans le dessein d'énoncer les forces et les faiblesses de leur utilisation comme moyen de preuve.

[908] BLUMSTEIN, p. 2; CORNU, p. 238.

I. Les techniques de la surveillance

1098 Les mesures de surveillance sont aujourd'hui reconnues comme des moyens d'investigation efficaces. Elles sont utilisées comme moyens de prévention, de répression ou de neutralisation, et sont susceptibles de satisfaire les exigences de fiabilité en tant que preuve.

1099 En s'appuyant sur les dispositions légales du Code de procédure pénale, la doctrine divise en deux catégories les techniques de surveillance liées aux nouvelles technologies[909]. D'une part, la surveillance par poste et télécommunication intègre les écoutes téléphoniques, l'interceptions des SMS ou e-mail. D'autre part, les autres moyens de surveillance permettent de capter des images et/ou d'enregistrer du son: il s'agit notamment de la vidéosurveillance.

1100 La présente partie traite de la surveillance des télécommunications (A.) entendue dans son sens large. Elle ne se restreint donc pas aux écoutes téléphoniques, mais à toute méthode permettant d'écouter, d'observer, d'enregistrer ou d'identifier un individu et pouvant servir dans l'administration des preuves[910]. La seconde partie analyse le cadre technique et juridique de la vidéosurveillance (B.).

A. La surveillance des télécommunications

1101 Depuis la fin de la seconde Guerre Mondiale, les télécommunications se sont démocratisées et partant, une recrudescence des infractions commises ou diligentées à l'aide de ce moyen de communication a été constatée. Pour contrer la criminalité, les autorités policières et judiciaires recourent alors aux mêmes moyens techniques de télécommunication pour investiguer[911].

[909] ALBERTINI, p. 53; HAUSER, SCHWERI, HARTMANN, p. 357-358 et 367; PIQUEREZ, Traité de procédure pénale suisse, p. 615 et 628; STRÄULI, p. 95 et 112.

[910] HUYGHE, Ecoutes téléphoniques, p. 3; PIQUEREZ, Traité de procédure pénale suisse, p. 612; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 438.

[911] BUQUET, p. 358; CONSEIL DE L'EUROPE, Surveillance, p. 5.

1. L'introduction

a. Définition de la surveillance de la correspondance par télécommunication

1102 La surveillance de la correspondance par poste et télécommunication est probablement la mesure de surveillance secrète la plus ancienne.

1103 La correspondance par télécommunication – qui nous intéresse dans la présente partie – se définit comme: "[...] l'émission ou la réception d'informations, sur des lignes ou par des ondes hertziennes, au moyen de signaux électroniques, magnétiques ou optiques ou d'autres signaux électromagnétiques" (art. 3 let. c LTC).

1104 Les écoutes téléphoniques ou la surveillance des moyens de télécommunication consistent à intercepter de manière secrète la correspondance téléphonique ou par messagerie pouvant prendre la forme orale, écrite ou imagée (art. 3 let. a LTC) et transmise par des installations fixes ou mobiles (art. 270 CPP)[912]. Il ne s'agit plus seulement d'écouter les communications téléphoniques, mais d'intercepter tout type de correspondances indépendamment des moyens de communication employés, ce qui inclut les données électroniques en voie de transmission[913].

1105 Ainsi, le pouvoir d'investigation de la police en matière de surveillance s'est élargi[914]. Il est dorénavant possible de surveiller un raccordement téléphonique fixe ou mobile et d'intercepter les SMS, MMS ou e-mail. Chacun de ces modes de raccordement est facilement identifiable. Le numéro d'appel identifie un raccordement de téléphonie fixe ou mobile, le numéro MSISDN, IMSI ou SIM individualise un raccordement à la téléphonie mobile, le numéro IMEI détermine un téléphone mobile et l'adresse IP personnalise le titulaire de l'accès internet.

b. Les deux types de surveillance des télécommunications

1106 Deux types de surveillance des télécommunications existent.

---

912 BIEDERMANN August, p. 80; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 441 et 447; RUCKSTUHL, p. 153; STRÄULI, p. 102.

913 CONSEIL DE L'EUROPE, Surveillance, p. 5; FRANCHIMONT, JACOBS, MASSET, p. 761; MOREILLON, BLANK, p. 89; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 441 et 443-444.

914 CORNU, p. 245; JEANNERET, KÜHN, p. 307; RUCKSTUHL, DITTMANN, ARNOLD, p. 261; STRÄULI, p. 103.

1107 La surveillance en temps réel est la forme classique de la surveillance. Elle se définit comme l'interception des transmissions permettant d'obtenir toutes les informations utiles à l'investigation – *Call Content* (CC) – (art. 16 let. a-c et 24*a* OSCPT). Le contenu de la correspondance échangée – contenu des conversations téléphoniques, des emails envoyés ou reçus en transmission, voire des SMS –, les données d'identification des correspondants – numéro de téléphone, numéro SIM, IMSI ou IMEI, adresse IP, adresse de messagerie électronique –, le moment et la durée de la conversation – date et heure des conversations ou des consultations des messages –, voire la localisation du téléphone mobile[915] lors de l'appel ou de l'envoi/réception du message sont considérés comme des informations utiles (art. 16 let. c OSCPT)[916].

1108 Une surveillance en temps réel peut également concerner les données accessoires relatives au trafic, à la facturation et à l'identification des usagers.

1109 La surveillance rétroactive consiste à recueillir les données liées aux trafics et à la facturation des communications – *Intercept Related Informations* (IRI) – sur les six derniers mois auprès du fournisseur du service de télécommunication ou d'internet (art. 273 CPP et art. 16 let. d et 24*b* OSCPT) ainsi que les informations d'identification[917]. Les données concernées sont de divers ordres: numéros appelés et reçus, date, heure et durée des communications, données relatives à la consultation des divers services de messageries vocale ou écrite, type de connexion internet, login, nom des usagers, etc. (art. 16 let. d et 24*b* OSCPT)[918].

1110 Notons encore que l'autorité policière ou d'instruction a la possibilité d'effectuer une demande de renseignements sur les divers types de raccordements de télécommunication (art. 14 LSCPT, art. 19 à 22 et 27 OSCPT). Non-constitutive d'une mesure de surveillance, la demande de renseignements est admissible à des conditions moins restrictives que la surveillance des télécommunications. Généralement connexe, il se peut qu'une demande de renseignements ne soit pas liée à une surveillance et serve uniquement à obtenir des informations sur le nom et l'adresse du titulaire du raccordement, de l'adresse de messagerie ou de l'accès Internet.

---

[915] Infra Partie II, Chapitre 3, II, n° 1673 ss.

[916] MOREILLON, BLANK, p. 88-89; PIQUEREZ, Traité de procédure pénale suisse, p. 617; SCHNEIDER, p. 187-188; STRÄULI, p. 104-105.

[917] BIEDERMANN August, p. 104-105; HANSJAKOB, BÜPF/VÜPF, art. 12 N 7-8; SCHNEIDER, p. 188 et 189.

[918] MÉTILLE, Thèse, p. 40; MOREILLON, BLANK, p. 89; SCHNEIDER, p. 188.

c. Le contexte technique de la surveillance des télécommunications

1111 La transmission téléphonique diffère selon le mode de téléphonie employé. Les communications émises depuis un téléphone fixe transitent par un câble de cuivre ou en fibre optique, par faisceaux hertziens ou par satellite. Les téléphones mobiles sont reliés quant à eux au réseau de téléphonie à l'aide des ondes radios. En outre, un appareil téléphonique standard n'est plus nécessaire pour communiquer, puisque les communications peuvent être transmises par le réseau électrique, le câble ou le réseau internet[919].

1112 Dépendamment du mode de transmission et du type de surveillance, les méthodes d'interception divergent.

1113 Généralement, le service Surveillance de la correspondance par poste et télécommunications (SCPT) chargé d'assurer la surveillance et de veiller au développement technologique se base sur les normes ou spécifications techniques de l'European Telecommunication Standard Institute (ETSI) pour la méthode à employer[920]. Actuellement, il existe encore quelques exceptions, principalement en ce qui concerne les mesures rétroactives pour lesquelles les données sont transmises de manière spécifique non-conforme aux standard ETSI. Néanmoins, de nouvelles directives sont en cours d'élaboration pour se conformer aux spécifications ETSI[921].

1114 Les normes ETSI étant des normes purement techniques qui n'ont pas, en soi, d'impact sur la valeur probatoire, nous ne nous attarderons pas plus sur la technicité de mise en œuvre de la surveillance des communications. Relevons simplement que pour permettre aux enquêteurs d'entendre directement les conversations, il est aujourd'hui possible de dévier le raccordement téléphonique ou l'accès internet directement aux postes de police[922].

---

[919] A ce sujet voir: HANSJAKOB, BÜPF/VÜPF, p. 39-51 et 60-64.

[920] A ce sujet voir: Lawful Interception (LI): Requirements for network functions – ETSI ES 201 158; Lawful Interception: Requirements for Law Enforcement Agencies (LEA) – ETSI TS 101 331; Lawful Interception (LI): Handover interface for the lawful interception of telecommunications traffic – ETSI TS 101 671; 3G security: Lawful interception architecture and functions – 3GPP TS 33.107, et Handover interface for Lawful Interception (LI) – 3GPP TS 33.108; Lawful Interception (LI): Handover Interface and Service-Specific Details (SSD) for IP delivery: Part 1-6 – ETSI TS 102 232-1, TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102-232-5 et 102 232-6; Lawful Interception (LI): Retained data handling: Handover interface for the request and delivery of retained data – ETSI TS 102 657.

[921] Informations obtenues par Monsieur Jean-Pascal CHAVANNE, Provider Management au Centre de services informatiques du Département fédéral de justice et police.

[922] CORNU, p. 245-246; CR-CPP-BACHER, ZUFFEREY, art. 270 N 1.

2. Le cadre légal

a. Les droits fondamentaux, les libertés et leur protection

1115 Les mesures techniques de surveillance s'immiscent immanquablement dans la vie privée des individus, dès lors qu'elles permettent d'obtenir des informations sur des conversations généralement privées. Ainsi, toutes ces mesures sont propres à porter atteinte aux droits fondamentaux.

i. La protection des communications et l'atteinte aux droits fondamentaux issus de la surveillance des télécommunications

1116 La protection des droits de la personnalité (art. 10 al. 2 Cst) et celle de la sphère privée (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 13 al. 1 Cst) confèrent à toute personne le droit de mener leur vie selon leurs propres choix[923].

1117 En matière de télécommunication, la protection de la sphère privée se comprend dans sa dimension de garantie de la vie privée et du respect des relations établies par les télécommunications. Ainsi, toute personne doit être en mesure de contrôler les informations non accessibles au public qui la concernent, et doit pouvoir transmettre librement des opinions et des informations à des personnes déterminées ou indéterminées, pouvoir en recevoir et avoir le droit au secret quant aux données que génèrent le traitement technique des communications.

1118 Relevons encore que la reconnaissance de la vie privée dans les télécommunications comme droit fondamental offre une confiance normale aux utilisateurs de pouvoir communiquer librement et en toute confidentialité. C'est cette même confiance qui est mise à mal par la surveillance des télécommunications[924].

1119 En outre, les normes fondamentales garantissent la protection contre l'emploi abusif des données (art. 13 al. 2 Cst), notamment celles relevant des télécommunications[925].

---

[923] ATF 118 IV 67, 70 = JdT 1994 IV 147, 148; ATF 126 I 50, 60-61 = JdT 2001 I 764, 773-774; ATF 130 III 28, 32-33; CourEDH, Affaire *Botta c. Italie*, arrêt du 24 février 1998, 21439/93, § 32; CourEDH, Affaire *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, 30562/04 et 30566/04, § 45; BARRELET, p. 41; BONDALLAZ, Jusletter, n° 11, 43, 46 et 58; CONSEIL DE L'EUROPE, Surveillance, p. 5; GIANNALOPOULOS, PARIZOT, p. 246; GRISEL E., p. 63; JEAN-RICHARD-DIT-BRESSEL, Mailbox, p. 167-168; MÜLLER, SCHEFER, p. 139-140; WALTER, p. 460-461 et 469.

[924] GIANNALOPOULOS, PARIZOT, p. 248.

[925] CORNU, p. 245-246; GRISEL E., p. 75-76; MÜLLER, SCHEFER, p. 171 ss.

1120 Les dispositions internationales ou constitutionnelles protégeant la vie et les échanges sociaux des individus couvrent l'ensemble des communications: orales, écrites, par voie postale, téléphonique ou réseau électrique. Par ailleurs, le Tribunal fédéral a confirmé que les messages électroniques – emails et messageries instantanées – et la téléphonie par Internet sont soumis au secret de la correspondance[926]. Indépendamment du mode de télécommunication, l'atteinte créée par la mesure d'investigation est d'une certaine intensité et est donc considérée comme une atteinte grave au droit au respect de la vie privée et de la correspondance[927].

1121 Peu importe que les mesures de surveillances portent atteinte aux libertés individuelles garanties par la liberté personnelle, la protection des données, du domicile ou autres droits, les autorités n'ont – en principe – par le droit de recourir à des mesures de surveillance. Cela étant, les droits individuels ne sont pas absolus.

ii. La restriction admissible des droits fondamentaux touchés par la surveillance secrète des télécommunications

1122 La restriction des droits personnels est envisageable.

1123 La Convention européenne des droits de l'Homme prévoit que l'ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée n'est admissible que si cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, etc. (art. 8 § 2 CEDH).

1124 Quant à la Constitution, elle exige pour limiter un droit fondamental : l'existence d'une base légale, une justification par un intérêt public ou par la protection d'un droit fondamental

[926] ATF 126 I 50, 65 = JdT 2001 I 764, 777-778; ATF 130 III 28, 32; ATF 140 IV 181, 184 = JdT 2015 IV 167, 169.
[927] ATF 109 Ia 273, 298-299 = JdT 1985 I 616, 618; ATF 122 I 182, 190 et 193 = JdT 1998 IV 58, 60; ATF 123 IV 236, 243-244 = JdT 1999 IV 176, 182-183; ATF 125 I 46, 49 = JdT 2000 IV 17, 19-20; ATF 125 I 96, 98 et 103 = JdT 2006 IV 28, 28 et 33-34; CourEDH, Affaire *Kopp c. Suisse*, arrêt du 25 mars 1998, 23224/94, § 72; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 56; BONDALLAZ, protection des personnes, p. 486; CR-CPP-BACHER, ZUFFEREY, art. 269 N 2; PIQUEREZ, Traité de procédure pénale suisse, p. 612.

d'autrui et la proportionnalité (art. 36 Cst)[928]. Il ne faut en outre pas perdre de vue que l'interception des conversations constitue un *ultimum remedium*[929].

1125 Au vu de la gravité de l'atteinte causée par la surveillance des télécommunications, ce moyen de contrainte doit reposer sur une base légale, être justifier par un intérêt public et respecter la proportionnalité (art. 36 Cst).

1126 Seule une base légale formelle revêtant une certaine clarté et précision peut justifier l'écoute des appels ou l'interception des messages (art. 36 al. 1 phr. 2 et 164 al. 1 let. b Cst)[930]. Le critère de précision doit cependant être modéré. L'évolution des technologies est telle qu'une précision trop importante provoquerait des lacunes pour certains domaines qui engendreraient des difficultés dans le travail d'investigation et d'administration des preuves[931].

1127 En droit suisse, la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT) dont la teneur a été en partie reprise dans le Code de procédure pénale fédéral (art. 269-298 CPP), ainsi que l'ordonnance relative à cette loi (OSCPT) fixent les conditions générales dans lesquelles une mesure de surveillance peut être ordonnée et exécutée. Ces bases légales constituent des normes législatives suffisantes – claires et précises – pour restreindre le secret des télécommunications et la sphère privée dans le cadre d'une procédure pénale[932].

1128 Le Tribunal fédéral a reconnu que le besoin d'ordre public et d'élucidation des infractions pénales pouvaient justifier la mise sous surveillance des télécommunications et respectaient

---

[928] AUBERT, MAHON, art. 36 N 7 ss; AUER, HOTTELIER, MALINVERNI, Vol. II, p. 77-117; BELSER, WALDMANN, MOLINARI, p. 145 ss; GOLDSCHMID, Überwachung, p. 23-42; HÄFELIN, HALLER, KELLER, p. 100-105; RHINOW, SCHEFER, p. 237-245; HALLER, p. 157-162.

[929] ATF 109 Ia 273, 287-288 = JdT 1985 I 616, 618; ATF 122 I 182, 187-188 = JdT 1998 IV 58; ATF 125 I 46, 47-48 = JdT 2000 IV 17, 18; ATF 126 I 50, 61 = JdT 2001 I 764, 773-774; ATF 128 I 327, 341 = JdT 2003 I 309, 321; CourEDH, Affaire *Valenzuela Contreras c. Espagne*, arrêt du 30 juillet 1998, 27671/95, § 46; CourEDH, Affaire *van Vondel c. Pays-Bas*, arrêt du 25 octobre 2007, 38258/03, § 50-54; CONSEIL DE L'EUROPE, Surveillance, p. 6; FRANCHIMONT, JACOBS, MASSET, p. 762; GIANNALOPOULOS, PARIZOT, p. 249; JEAN-RICHARD-DIT-BRESSEL, Mailbox, p. 168; JOBARD, SCHULZE-ICKING, p. 63; PIQUEREZ, Traité de procédure pénale suisse, p. 612-613; RUCKSTUHL, p. 154.

[930] ATF 109 Ia 273, 282-284 = JdT 1985 I 616, 617; ATF 125 I 96, 98 = JdT 2006 IV 28, 29; ATF 126 I 50, 61 = JdT 2001 I 764, 773-774; CourEDH, Affaire, *Malone c. Royaume-Uni*, arrêt du 2 août 1984, 8691/79, § 67; CourEDH, Affaire *Valenzuela Contreras c. Espagne*, arrêt du 30 juillet 1998, 27671/95, § 46.

[931] ATF 109 Ia 273, 286 = JdT 1985 I 616, 617-618.

[932] BONDALLAZ, protection des personnes, p. 508.

par conséquent la condition d'intérêt public[933]. En effet, les moyens de surveillance des télécommunications sont des méthodes d'investigation efficaces pour garantir la sécurité publique et pour poursuivre les infractions pénales[934], en étant utilisées comme moyen de preuve à charge ou à décharge.

1129 La proportionnalité demande que la surveillance des télécommunications soit apte à atteindre le but de sécurité et ordre public, soit nécessaire et respecte un équilibre entre les intérêts des particuliers et celui de l'Etat[935]. Ainsi, la mesure d'investigation doit être réellement efficace pour atteindre le but désiré, ce qui est largement démontré surtout en cas de surveillance d'un suspect. L'établissement des faits ne doit en outre pas être possible par un autre moyen d'investigation. La mesure de surveillance doit également être justifiée notamment par la gravité de l'infraction ou de la menace pour la sécurité publique. Cette dernière condition est remplie dès lors que les dispositions légales relatives à la surveillance des télécommunications définissent le cadre de la mise sous surveillance en la limitant notamment à une liste exhaustive d'infractions susceptibles de motiver une telle mesure en temps réel ou en limitant l'usage de la mesure rétroactive pour élucider un crime, un délit ou une contravention au sens de l'art. 179*septies* CP. Nous ne nous étendrons pas ici sur ces dispositions qui font l'objet d'un développement distinct[936].

1130 Au surplus, la jurisprudence de la Cour européenne et du Tribunal fédéral précisent certaines exigences que les mesures de surveillance doivent respecter pour que l'atteinte aux droits fondamentaux soit admissible[937]. Toute surveillance doit être autorisée par un juge, mais la surveillance générale et/ou préventive n'est pas autorisable. La base légale autorisant la surveillance doit être accessible aux citoyens qui doivent pouvoir prévoir les circonstances dans lesquelles une telle mesure d'investigation peut être mise en place. Par exemple, en l'état actuel de la législation, l'introduction d'un cheval de Troie dans un ordinateur protégé

---

933 ATF 109 Ia 273, 287-288 = JdT 1985 I 616, 618; ATF 128 I 327, 341 = JdT 2003 I 309, 321; BONDALLAZ, Jusletter, n° 13; BONDALLAZ, protection des personnes, p. 490; GIANNALOPOULOS, PARIZOT, p. 248-249; HUYGHE, Ecoutes téléphoniques, p. 39; JOBARD, SCHULZE-ICKING, p. 63; RUCKSTUHL, p. 154; SCHNEIDER, p. 180.

934 BONDALLAZ, protection des personnes, p. 485; STRÄULI, p. 123.

935 ATF 109 Ia 273, 287-288 = JdT 1985 I 616, 618; ATF 128 I 327, 341 = JdT 2003 I 309, 321; BONDALLAZ, Jusletter, n° 13; BONDALLAZ, protection des personnes, p. 490; GIANNALOPOULOS, PARIZOT, p. 248-249; HUYGHE, Ecoutes téléphoniques, p. 39; JOBARD, SCHULZE-ICKING, p. 63; RUCKSTUHL, p. 154; SCHNEIDER, p. 180.

936 Infra Partie II, Chapitre 3, I, A, 2, c, n° 1140 ss.

937 ATF 120 Ia 314, 317-319; ATF 122 I 182, 187- 189 = JdT 1998 IV 58; ATF 125 I 96, 103 = JdT 2006 IV 28, 33-34; ATF 133 IV 182, 183-184; TF 1B_226/2010 du 23 juillet 2010, c 2.2-2.3; CourEDH, Affaire *Klass et autres c. Allemagne*, arrêt du 6 septembre 1978, 5029/71, § 43 et 51; CourEDH, Affaire *Kruslin c. France*, arrêt du 24 avril 1990, 11801/85, § 27 et 33; CourEDH, Affaire *Popescu c. Roumanie*, arrêt du 25 novembre 2003, 38360/97, § 79; CourEDH, Affaire *Natunen c. Finlande*, arrêt du 31 mars 2009, 21022/04, § 39 et 42.

pour le surveiller ne paraît pas être admissible[938]. A noter que la prévisibilité normative doit permettre de remplir la condition de finalité de la mesure de contrainte axée sur la confirmation des soupçons et non leur création[939]. Pour finir, un certain nombre de droits doivent être garantis: droit de consulter les enregistrements, durée limitée de conservation des informations, droit de recours devant une autorité judiciaire indépendante et impartiale, etc.

b. La protection du Code pénal

i. Les infractions du Code pénal

1131 Le Code pénal protège explicitement le secret de la correspondance et des télécommunications en réprimant la divulgation de renseignements à des tiers par les fonctionnaires, employés ou auxiliaires des services postaux ou de télécommunication (art. 321*ter* CP). Quant aux écoutes et/ou l'enregistrement non-autorisé d'une conversation non publique, elles font également l'objet d'une infraction pénale (art. 179*bis* et 179*ter* CP).

1132 Les écoutes des communications de téléphonie fixe, mobile ou VoIP[940] doivent donc être justifiées pour ne pas enfreindre la loi pénale. La surveillance officielle par une autorité pénale peut être licite de par la loi (art. 179*octies* CP et art. 269ss CPP). L'interception des écoutes téléphonique par des particuliers peut, quant à elle, se justifier par la légitime défense (art. 15 CP) – par exemple, en cas de riposte à une injure ou une diffamation – ou par l'état de nécessité[941].

1133 A noter que le terme "*conversation*" utilisé dans les bases légales précitées suppose un entretien oral de vive voix ou par l'entremise d'un téléphone entre deux personnes au moins, ce qui exclut tout type d'écrit, notamment les SMS ou les emails.

1134 A l'instar des art. 179*bis* et 179*ter* CP, l'art. 179 CP ne réprime pas non plus l'interception des emails, et donc, par analogie, des SMS à défaut d'être en présence de pli fermé et donc

---

[938] HANSJAKOB, GovWare, n° 16; Message, P-LSCPT, p. 2398 et 2467-2468; RISS, ZANON, n° 30; TRECCANI, p. 225-227. Infra Partie II, Chapitre 3, I, A, 4, c, n° 1306 ss.

[939] MÉTILLE, Thèse, p. 118; BÉNÉDICT, p. 210.

[940] Infra Partie II, Chapitre 3, I, A, 4, c, i, n° 1304 ss.

[941] GAUTHIER, Enregistrement clandestin, p. 337; HURTADO POZO, art. 179*bis* N 2213; SCHMID, Handbuch, p. 364-365; SCHUBARTH, Strafrecht, art. 179 N 39 et art. 179*bis* N 40.

d'être protégé contre les accès indus de tiers[942]. Notons encore qu'un mot de passe ou un code ne suffit pas à reconnaître la protection suffisante comparable à un pli fermé.

1135 Sous couvert du respect des droits fondamentaux, les autorités d'investigation et de poursuite ne sont toutefois pas libres de surveiller les télécommunications par SMS ou emails, et doivent respecter la procédure (art. 269 ss CPP). En revanche, hormis les cas où le comportement tombe sous le coup des art. 143 et 143*bis* CP, la preuve apportée par un particulier qui a intercepté un ou plusieurs SMS ou emails semble pouvoir être recevable sans motif justificatif car pénalement atypique.

ii. L'exclusion de l'application des art. 179bis et ter CP

1136 En procédure pénale, les mesures d'investigations secrètes incluant la surveillance des télécommunications sont des moyens de contrainte essentiels, notamment pour lutter contre le crime organisé. Il est par conséquent nécessaire que l'autorité pénale puisse bénéficier de cette mesure de contrainte.

1137 Bien que le titre marginal de l'art. 179*octies* CP parle d'exemption de peine, cet article décrit un comportement non punissable. Par conséquent, quiconque se conforme à cette base légale agit licitement au sens de l'art. 14 CP puisque la loi autorise le comportement.

1138 Dans le respect des normes pénales, l'autorité désireuse de mettre en œuvre une surveillance des télécommunications doit l'exercer dans une attribution conférée par la loi et obtenir l'autorisation d'un juge (art. 179*octies* CP). Lorsque les deux conditions sont remplies, la surveillance n'est pas punissable et l'acte ne constitue donc pas une infraction.

1139 Il appartient par conséquent aux lois de procédure de déterminer quelles sont les personnes qui peuvent ordonner une mesure de surveillance et sous quelles conditions l'approbation du juge peut être accordée.

[942] ATF 126 I 50, 65 = JdT 2001 I 764, 778; ATF 130 III 28, 32; DONATSCH, Strafrecht, p. 397; HURTADO POZO, art. 179 N 2176.

c. Les normes fédérales élémentaires à la surveillance répressive des télécommunications

1140 Les mesures de surveillances, plus spécifiquement les mesures consacrées à la surveillance par poste et télécommunication sont définies aux articles 269-279 CPP. Ces dispositions abrogent les art. 3 à 10 aLSCPT dont elles s'inspirent largement. Afin d'harmoniser les procédures de mise en œuvre des mesures de contrainte et pour clarifier certains points, voire remédier aux défauts de l'aLSCPT, quelques différences existent néanmoins entre les conditions de mises sous surveillance anciennement prévues par la LSCPT et celles du CPP[943].

1141 Notons encore qu'à défaut de base légale prévoyant la procédure d'exécution ou de contrôle de la surveillance dans le CPP, la LSCPT reste en vigueur sur ces points.

i. Le champ d'application

1142 Les art. 269 ss CPP s'appliquent pour toutes les surveillances des correspondances qui sont ordonnées et exécutées dans le cadre d'une procédure pénale fédérale ou cantonale pendante, exception faite des cas de recherche d'urgence des personnes disparues (art. 1 al. 1 let. c et 3 LSCPT). Par renvoi, elles peuvent également être exécutées dans le cadre d'une demande d'entraide pénale (art. 1 al. 1 let. a et b LSCPT).

1143 Le Code de procédure pénale, contrairement aux législations cantonales en matière de police, ne prévoit en revanche pas la possibilité d'effectuer une surveillance préventive[944]. Cette interdiction doit toutefois être nuancée. Lorsque la surveillance peut prévenir indirectement une infraction, notamment lorsque l'activité délictueuse se poursuit dans la durée[945], ou qu'elle permet d'élucider des infractions futures, notamment pour prouver la réalisation de l'aggravante du métier[946], elle peut être licite. En effet, les informations obtenues concernent bien de futures infractions, mais la mesure de contrainte permet en premier lieu de mettre un terme aux activités délictueuses[947].

---

[943] CR-CPP-BACHER, ZUFFEREY, art. 269-281 N 2.

[944] HANSJAKOB, BÜPF/VÜPF, art. 1 N 4; SCHMID, Praxiskommentar, art. 269 N 7.

[945] HANSJAKOB, BÜPF/VÜPF, art. 1 N 4; OBERHOLZER, Strafprozessrechts, p. 420; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 446; SCHMID, Praxiskommentar, art. 269 N 6-7.

[946] Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 446.

[947] HANSJAKOB, BÜPF/VÜPF, art. 3 N 4.

1144 En outre, la législation fédérale autorisant la surveillance que dans le cadre d'une procédure pénale pendante, la surveillance d'un condamné après l'entrée en force du jugement – que ce soit en cas d'évasion ou pour débuter sa peine – n'est pas admis par le Code de procédure pénale[948]. En effet, une telle surveillance est une pure mesure de police relevant de la compétence des cantons.

ii. Les conditions d'application

a) Pour la surveillance des communications

1145 Dans le cadre de la surveillance en temps réel du contenu des communications, l'art. 269 CPP prévoit quatre conditions cumulatives pour qu'une surveillance puisse être ordonnée.

1. L'existence de graves soupçons

1146 Afin de respecter la présomption d'innocence, l'autorisation de la surveillance dépend tout d'abord de la présence de graves soupçons pesant sur la personne dont le raccordement doit être surveillé suite à un comportement punissable et prévu dans la liste exhaustive des infractions (art. 197 al. 1 let. b CPP et 269 al. 1 let. a et al. 2 CPP). La notion de "*graves soupçons*" s'entend autant en lien avec une infraction consommée, tentée, de commission ou d'omission, intentionnelle ou par négligence[949].

1147 Une prévention suffisante existe lorsque les soupçons ont atteint une certaine intensité comparativement au "*fortement soupçonné*" de l'art. 221 al. 1 CPP justifiant la mise en détention provisoire. En théorie, seule la gravité objective de l'infraction et la probabilité que le ou les auteurs utilisent un moyen de communication pour commettre le forfait sont les critères déterminants pour faire figurer une infraction dans la liste[950]. Quant à la notion de "*graves soupçons*" – simple rappel d'une des conditions de principe des mesures de contrainte (art. 197 al. 1 let. b CPP) –, elle se réfère à l'intensité des indices concrets que la personne concernée par la surveillance du raccordement a commis l'une des infractions autorisant la

[948] EICKER, HUBER, p. 181; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 441-442; SCHMID, Praxiskommentar, art. 269-279 N 2; StPO-HANSJAKOB, art. 269 N 4.

[949] CR-CPP-BACHER, ZUFFEREY, art. 269 N 7; HANSJAKOB, BÜPF/VÜPF, art. 3 N 13 et 15; JEANNERET, KÜHN, p. 310; PERRIER, VUILLE, p. 163.

[950] CR-CPP-BACHER, ZUFFEREY, art. 269 N 8 et 22; SCHMID, Praxiskommentar, art. 269 N 8-9; StPO-HANSJAKOB, art. 269 N 22 et 30.

surveillance[951]. En somme, les charges reposant sur les faits, des déclarations de témoins ou d'autres sources doivent être vérifiables et donc objectivement fondées pour permettre la surveillance[952].

1148 A noter que les exigences sont nettement moindres en ce qui concerne la surveillance dite rétroactive, étant donné que le contenu de la surveillance n'est pas connu et donc que l'atteinte aux droits fondamentaux est de moindre importance.

1149 La nécessité d'avoir des soupçons importants permet de respecter tant le principe de proportionnalité que de prévisibilité. L'accomplissement de la première condition assure en outre une limitation suffisante contre les opérations de *fishing expeditions* et évite que le CPP puisse servir de base légale à une mesure de surveillance préventive qui sort du cadre de cette loi[953].

2. La justification au regard de la gravité de l'infraction

1150 La seconde condition (art. 197 al. 1 let. c et 269 al. 1 let. b CPP) de mise en œuvre de la surveillance répond à la nécessité de poursuivre un intérêt public prépondérant.

1151 L'atteinte à la sphère privée et au respect de la correspondance étant grave, la proportionnalité de la mesure de contrainte ne doit faire aucun doute dans les circonstances du cas d'espèce. Ainsi, le ministère public doit mettre en balance la nature du bien juridique atteint par l'acte délictuel, la gravité de l'atteinte, le *modus operandi*, l'intensité délictueuse, les mobiles de l'auteur ou encore la finalité de son acte[954].

1152 Au surplus, la mesure de surveillance doit être également adéquate[955]. Elle ne se justifie que si elle est propre à obtenir des résultats concrets que nulle autre mesure moins invasive ne peut atteindre[956].

---

951 ATF 141 IV 459, 462; TF 1B_230/2013 du 26 juillet 2013, c. 5.1.1; BIEDERMANN August, p. 83; SCHMID, Praxiskommentar, art. 269 N 6.

952 ATF 109 Ia 273, 287-288 = JdT 1985 I 616, 618; ATF 128 I 327, 341 = JdT 2003 I 309, 321; HANSJAKOB, BÜPF/VÜPF, art. 3 N 10; JEANNERET, KÜHN, p. 311;.

953 Message, CPP, p. 1235.

954 HANSJAKOB, BÜPF/VÜPF, art. 3 N 18 ss; STRÄULI, p. 128.

955 ATF 141 IV 459, 461; CR-CPP-BACHER, ZUFFEREY, art. 269 N 11 ss; MOREILLON, PAREIN-REYMOND, art. 269 N 7.

956 BSK-StPO-RICHARD-DIT-BRESSEL, art. 269, N 47; CR-CPP-BACHER, ZUFFEREY, art. 269 N 16 et 18; HANSJAKOB, BÜPF/VÜPF, art. 3 N 25-26 et 34; Message, LSCPT, p. 3711; MOREILLON, PAREIN-REYMOND, art. 269 N 7.

1153 Enfin, l'intérêt public doit l'emporter sur l'atteinte à la sphère privée et aux libertés personnelles touchées par la mesure de contrainte.

3. La subsidiarité de la mesure

1154 La mesure de surveillance des télécommunications est l'*ultima ratio* (art. 197 al. 1 let. d et 269 al. 1 let. c CPP).

1155 Cependant, il n'est pas utile que l'autorité d'enquête utilise, préalablement à la mise en œuvre de la surveillance, une autre technique[957]. En effet, il suffit qu'il soit reconnu que, sans la surveillance, les recherches ne fourniraient aucune indication ou qu'elles seraient compliquées.

4. Le catalogue limitatif des infractions susceptibles de justifier une surveillance

1156 Alors qu'elle est édictée au deuxième alinéa de l'art. 269 CPP, la quatrième condition est en réalité la première condition examinée par le ministère public, ou tout du moins, elle l'est en parallèle de la condition de graves soupçons.

1157 Le catalogue limitatif des infractions pouvant justifier la surveillance des télécommunications (art. 269 al. 2 CPP) est exhaustif[958]. Vraisemblablement, la gravité objective d'une infraction et la probabilité qu'un auteur utilise un moyen de télécommunication pour perpétrer son acte délictuel devrait fonder les critères pour qu'une infraction figure dans le catalogue de l'art. 269 al. 2 CPP.

1158 Malgré les modifications apportées dans le CPP à la liste des infractions, la doctrine reste critique sur certaines incohérences dans le catalogue des infractions ou sur l'absence de certains actes délictuels[959].

---

957 ATF 141 IV 459, 462; JEANNERET, KÜHN, p. 311; MOREILLON, PAREIN-REYMOND, art. 269 N 8; PERRIER, VUILLE, p. 163; SCHMID, Praxiskommentar, art. 269 N 11; STRÄULI, p. 129;.

958 TF 6S.488/2004 du 12 mai 2005, c. 1.1.

959 A ce sujet voir: CR-CPP-BACHER, ZUFFEREY, art. 269 N 24 ss; JEAN-RICHARD-DIT-BRESSEL, Mailbox, p. 67; STRÄULI, p. 125.

b) Pour l'obtention des données relatives au trafic et à la facturation et identification des usagers

1159 Concernant la surveillance rétroactive et réelle des données dites accessoires (art. 273 CPP), la surveillance étant moins invasive, les conditions d'admissibilité de la mesure sont moins restrictives[960]. L'accès aux données peut en effet être ordonné en dehors de la commission des infractions listées à l'art. 269 al. 2 CPP.

1160 Le ministère public peut demander que lui soient fournies les données lorsque des graves soupçons laissent présumer qu'un crime, un délit ou une contravention au sens de l'art. 179*septies* CP (art. 273 al. 1 CPP) a été commis. Le catalogue des infractions justifiant la mesure est donc plus large que pour la surveillance des communications. En revanche, la notion de "*graves soupçons*" est identique à ce qui prévaut pour l'art. 269 CPP.

1161 Au surplus, corrélativement à la surveillance en temps réel du contenu de la communication, le ministère public doit vérifier que les conditions de 269 al. 1 let. b et c CPP sont remplies.

iii. Les objets de la surveillance de la correspondance par télécommunication

1162 Comme précédemment énoncé[961], tous les types de correspondances sont concernés par la surveillance secrète par poste et télécommunications: ligne fixe ou mobile, bipeur, connexion internet, etc. L'objet de la surveillance des télécommunications est par conséquent large.

1163 Au sens de l'art. 270 CPP, la surveillance doit notamment porter sur un raccordement de télécommunication. Les fournisseurs des systèmes de télécommunication dans leur ensemble sont donc concernés par l'application d'une surveillance des correspondances, notamment les entreprises soumises à concession ou à l'obligation d'annoncer qui fournissent des raccordements téléphoniques ou des accès à Internet (art. 1 al. 2 LSCPT)[962].

1164 L'art. 270 CPP détermine en outre quels raccordements de télécommunication peuvent être surveillés.

1165 En premier lieu, la surveillance peut être ordonnée dans un but d'investigation contre un prévenu. Le prévenu (art. 111 CPP) est la personne contre laquelle il existe de graves

[960] ATF 139 IV 98, 99 = JdT 2014 IV 3, 4; JEANNERET, KÜHN, p. 312; MOREILLON, PAREIN-REYMOND, art. 273 N 2; PERRIER DEPEURSINGE, art. 269, p. 351.

[961] Supra Partie II, Chapitre 3, I, A, 1, a, n° 1105.

[962] BIEDERMANN August, p. 79; STRÄULI, p. 95.

soupçons de commission d'un certain type d'infraction – surveillance rétroactive ou en temps réel pour les données accessoires – ou d'une infraction listée – surveillance en temps réel des communications – en tant que participant principal ou accessoire[963].

1166 Cette définition constitue une limite suffisante contre les *fishing expeditions*. Elle exclut également les possibilités de surveiller des auteurs inconnus non-individualisables.

1167 Par contre, la surveillance d'un raccordement d'un auteur non-identifiable mais individualisable est possible s'il est prouvé que l'utilisateur du téléphone – par exemple, du téléphone mobile – est probablement l'auteur d'une infraction[964]. Dès lors, ce qui importe c'est que le prévenu soit le titulaire ou le co-titulaire et fasse lui-même usage du raccordement devant être mis sous surveillance.

1168 En second lieu, le raccordement d'un tiers peut faire l'objet d'une surveillance dans deux cas de figure: le prévenu utilise le raccordement comme s'il s'agissait du sien (art. 270 let. b ch. 1 CPP), ou le tiers reçoit des communications pour le compte du prévenu ou de la part de ce dernier (art. 270 let. b ch. 2 CPP)[965].

1169 Pour surveiller le raccordement d'un tiers, il est obligatoire que l'autorité ait des indices objectifs laissant penser que le prévenu en fait usage soit directement, soit indirectement ou par personne interposée[966]. A cet égard, le Tribunal fédéral a estimé que le raccordement d'une partie plaignante pouvait faire l'objet d'une surveillance rétroactive, si tant est que les données servent directement à l'élucidation de l'infraction[967].

1170 En outre, bien que le CPP ne l'exprime pas explicitement, les raccordements publics – cabines téléphoniques notamment – ou anonymes – carte SIM au nom d'autrui, par exemple

[963] CR-CPP-BACHER, ZUFFEREY, art. 269 N 10; STRÄULI, p. 131.

[964] CR-CPP-BACHER, ZUFFEREY, art. 270 N 7; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 258; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 448.

[965] ATF 138 IV 232, 234 et 239 = JdT 2013 IV 200; TF 1B_563/2012 du 6 novembre 2012, c. 4 et 6.1-6.2; TPF 2007 13, 14-15; BIEDERMANN August, p. 84; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 229; JEANNERET, KÜHN, p. 310; PERRIER DEPEURSINGE, art. 270, p. 353-354; PIQUEREZ, Traité de procédure pénale suisse, p. 621; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 448; RIEDO, FIOLKA, NIGGLI, p. 320; STRÄULI, p. 133-135. *A contrario* HANSJAKOB, BÜPF/VÜPF, art. 4 N 10.

[966] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 258; JEAN-RICHARD-DIT-BRESSEL, BÜPF, p. 47; Message, CPP, p. 1231; STRÄULI, p. 134-135.

[967] ATF 142 IV 34, 39-41.

d'une entreprise – sont assimilables aux raccordements de tiers[968]. La surveillance de ces derniers raccordements pouvant toucher la sphère privée d'un nombre conséquent de personnes, le ministère public est en droit, voire dans l'obligation, de ne pas exploiter les données dont la voix n'est pas identifiable comme celle du ou des prévenus, ou de tiers en lien avec l'enquête[969].

iv. La procédure de mise sous surveillance des télécommunications

a) Les compétences pour ordonner et autoriser la mesure de surveillance

1171 En toute hypothèse – surveillance en temps réel ou rétroactive–, le ministère public est compétent pour ordonner la surveillance des télécommunications (art. 269 al. 1 CPP) et/ou pour obtenir les données relatives au trafic, à la facturation et à l'identification des usagers (art. 273 al. 1 CPP).

1172 La transmission des communications et la collecte des données accessoires constituant une ingérence plus ou moins grave à la sphère privée des individus, l'ordre de surveillance doit être avalisé par une autorité judiciaire indépendante. La compétence pour autoriser une surveillance est confiée au tribunal des mesures de contrainte (art. 18, 272 al. 1, 273 al. 2 et 274 CPP).

b) La procédure d'autorisation et autorisation-cadre

1173 La surveillance des télécommunications débute par l'ordre donné par le ministère public sous forme d'une décision faisant généralement suite à la requête des enquêteurs et sur la base du rapport de police. A noter qu'à ce stade, aucune motivation n'est exigée pour ordonner la surveillance.

1174 L'ordre de surveillance – contenant toutes les informations nécessaires pour mettre en œuvre la surveillance (art. 15 et 23 OSCPT) – est alors adressé par poste, télécopie ou par tout moyen de transmission sécurisé, voire oralement en cas d'urgence au SCPT qui fait office d'autorité intermédiaire entre les divers fournisseurs existants et les organes de poursuite ou d'instruction pénale (art. 5 al. 1 OSCPT).

---

[968] CR-CPP-BACHER, ZUFFEREY, art. 270 N 16; Message, CPP, p. 1231; MÉTILLE, Thèse, p. 170; PERRIER, VUILLE, p. 163; PIQUEREZ, Traité de procédure pénale suisse, p. 621; PITTELOUD, p. 446; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 448.

[969] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 259.

1175 Même si elle est directement exécutoire, la décision du ministère public a une durée de validité limitée à vingt-quatre heures, calculée à la minute près. Dans ce délai, qui commence à courir dès la transmission de l'ordre de surveillance au SCPT, le ministère public doit requérir l'autorisation de surveillance auprès du tribunal des mesures de contrainte (art. 274 al. 1 CPP).

1176 Le régime d'autorisation (art. 273 al. 2 et 274 CPP) assure une meilleure protection des personnes concernées par la surveillance. En effet, la mesure de contrainte étant effectuée secrètement et s'immisçant dans la vie sociale des individus, la personne concernée ne peut pas recourir immédiatement contre la décision du ministère public[970]. Grâce à la validation ou invalidation de l'ordre par une autorité judiciaire, deux autorités vérifient le respect des conditions de mise sous surveillance ce qui doit permettre d'éviter les abus.

1177 A ce stade de la procédure de mise sous surveillance, la demande de l'autorité chargée de l'enquête doit contenir un exposé des motifs en fait et en droit qui explique notamment en quoi les conditions de mises sous surveillance sont données et pourquoi tel ou tel raccordement doit être surveillé (art. 274 al. 1 let. b CPP). Si l'individu concerné par la surveillance change de raccordement à intervalles rapprochés – à partir de trois changements ou usage de trois numéros aux cours des derniers mois[971] –, une autorisation-cadre peut être demandée (art. 272 al. 2 CPP), ce qui réduit notablement les charges administratives de l'autorité chargée de l'enquête.

1178 En outre, pour étayer sa demande, le ministère public fournit les éléments de preuve sur lesquels il s'est fondé pour ordonner la surveillance, ainsi qu'éventuellement les éléments recueillis durant les premières vingt-quatre heures[972].

1179 La décision d'autorisation intervient après vérification par le tribunal des mesures de contrainte du respect des conditions de l'art. 269 CPP, mais non de son opportunité[973]. La Cour rend sa décision sous forme d'une ordonnance écrite et motivée dans les cinq jours qui suivent la transmission de l'ordre de surveillance au SCPT. Etant précisé que le premier jour n'est pas compté (art. 44 al. 1 LTF) et que le délai est respecté si la décision d'autorisation est transmise et non reçue dans les cinq jours.

---

[970] Message, LSCPT, p. 3691.

[971] HANSJAKOB, BÜPF/VÜPF, art. 4 N 37; JEANNERET, KÜHN, p. 313; SCHMID, Praxiskommentar, art. 271 N 4.

[972] STRÄULI, p. 144.

[973] CR-CPP-BACHER, ZUFFEREY, art. 274 N 9.

1180 Le tribunal des mesures de contrainte peut approuver ou refuser la mesure de surveillance. En cas d'autorisation, l'exécution de la mesure peut naturellement se poursuivre, alors qu'en cas de refus d'autoriser la surveillance, la mesure de contrainte doit immédiatement cesser. Le ministère public doit, dans ce cas, communiquer au prévenu ainsi qu'aux tiers ayant fait l'objet d'une surveillance les motifs, le mode et la durée de la surveillance (art. 279 al. 1 CPP)[974].

1181 Relevons encore que le tribunal des mesures de contrainte peut également assortir sa décision de conditions, approuver provisoirement la mesure ou demander des compléments (art. 274 al. 2 CPP). Il peut en outre indiquer si des mesures spécifiques visant à sauvegarder le secret professionnel doivent être prises, voire si la possibilité d'un branchement direct est acceptable (art. 274 al. 4 CPP). Dans ces hypothèses, la motivation de la décision d'autorisation est accrue[975].

1182 En complément de la surveillance, une demande de renseignements est souvent formulée (art. 14 LSCPT et art. 19-22 et 27 OSCPT). Ceci permet à l'autorité d'investigation et judiciaire d'identifier le ou les titulaires de numéros téléphoniques ou d'adresses électroniques.

c) L'exécution de la mesure

1. Le Service de surveillance de la correspondance par poste et télécommunication (SCPT)

1183 L'organe d'exécution de la surveillance de la correspondance fait exception aux autres mesures de contrainte. Alors qu'en règle générale, la police est chargée d'exécuter ces mesures, la LSCPT donne la compétence au SCPT rattaché administrativement au DFJP (art. 2 al. 1 LSCPT et art. 3 al. 1 OSCPT).

1184 Après s'être assuré notamment que l'acte délictuel fait partie de la liste des infractions concernées par la surveillance des télécommunications et que l'ordre émane du ministère public (art. 13 al. 1 let. a LSCPT), le SCPT donne suite à l'ordre de surveillance. L'examen de l'ordre de surveillance est purement formel et ne saurait être le lieu d'un contrôle des

[974] Infra Partie II, Chapitre 3, I, A, 2, c, iv, e) , n° 1197 ss.

[975] HANSJAKOB, BÜPF/VÜPF, art. 7 N 19.

conditions normatives, notamment la subsidiarité ou la proportionnalité[976]. Le service n'a donc qu'un rôle d'exécutant[977].

1185 En revanche, si le SCPT constate un vice dans la décision du ministère public, il en informe directement l'autorité judiciaire et, au besoin, demande qu'aucune donnée ne soit transmise par les fournisseurs de services de télécommunications et/ou d'accès internet (art. 13 al. 1 let. a LSCPT).

1186 Avant ou après autorisation de la surveillance, le SCPT détermine quelles mesures d'ordre technique et organisationnel doivent être mises en œuvre dans le cas particulier (art. 13 al. 1 let. b LSCPT et 17 al. 1 et 25 al. 1 OSCPT). Il communique les directives aux fournisseurs de services (art. 13 al. 1 let. b LSCPT).

1187 En outre, le SCPT reçoit par déviation les communications qui transitent par le raccordement ou l'accès internet surveillé (art. 13 al. 1 let. c LSCPT). Cette mesure permet au service d'enregistrer les communications et les données de facturation utiles à la surveillance sur des supports de données ou des documents qu'il transmet au ministère public. Il réceptionne également les données accessoires relatives au trafic, à la facturation et à l'identification des usagers (art. 13 al. 1 let. e LSCPT). Lors d'un branchement direct, il veille à son installation mais n'enregistre en aucun cas les communications (art. 13 al. 1 let. d). Pour le surplus, il veille à la bonne exécution de l'ordre et de l'autorisation de surveillance.

2. Les fournisseurs de services de télécommunication et d'accès internet

1188 Les fournisseurs de services de télécommunication, d'accès internet, voire les hébergeurs[978] sont les deuxièmes acteurs de l'exécution de la mesure de surveillance des télécommunications. C'est à eux que revient l'exécution des mesures techniques contenue dans la directive du SCPT.

1189 En outre, ils doivent assumer un certain nombre d'obligations. Leur principale tâche est de retenir les informations du raccordement surveillé – surveillance en temps réel –, conserver les données relatives au trafic et à la facturation durant six mois – surveillance dite rétroactive – et transmettre au SCPT toutes les informations nécessaires à l'enquête (art. 15 al. 1 LSCPT).

---

[976] ATF 130 II 249, 253-254; HANSJAKOB, BÜPF/VÜPF, art. 11 N 2; JEANNERET, KÜHN, p. 315; HEINIGER, n° 8-9; Message, LSCPT, p. 4241; PITTELOUD, p. 446.

[977] ATF 130 II 249, 254; JEANNERET, KÜHN, p. 315; PITTELOUD, p. 446.

[978] TF 6B_766/2009 du 8 janvier 2009, c. 3.4.

1190 Corrélativement à ce qui prévaut pour le SCPT, les fournisseurs de services de télécommunication n'ont pas le pouvoir de contester la légalité d'une mesure de surveillance ou encore son opportunité[979]. Ils ne sont donc également que des exécutants et sont obligés de transmettre les informations couvertes par un ordre de surveillance.

d) La levée de la surveillance

1191 L'exécution de la mesure de surveillance, corrélativement la mesure elle-même, prend fin immédiatement lorsque le ministère public renonce à l'exécution, les conditions requises pour l'application de la mesure ne sont plus remplies (art. 275 al. 1 let. a CPP) – par exemple parce que la surveillance a permis d'écarter les graves soupçons initiaux ou parce que l'infraction considérée est hors liste – ou parce que les conditions procédurales n'ont pas été respectées, voire parce que l'autorisation a été refusée (art. 275 al. 1 let. b CPP).

1192 En dehors de ces hypothèses, l'autorisation pour la surveillance en temps réel est octroyée durant trois mois à compter de sa mise en œuvre technique et se compte à la minute près (art. 274 al. 5 CPP)[980]. Cependant, pour autant que la proportionnalité soit respectée et que la demande de prolongation soit motivée par le ministère public (art. 274 al. 5 CPP), un renouvellement de l'autorisation est possible pour des périodes de trois mois.

1193 En outre, lorsque les soupçons sont confirmés et qu'il existe suffisamment d'éléments pour justifier une arrestation, l'autorité d'enquête doit intervenir et la surveillance est, par conséquent, interrompue.

1194 Pour ce qui concerne la surveillance rétroactive, l'art. 273 al. 3 CPP prévoit l'obtention des informations pouvant avoir six mois d'ancienneté. Ce délai semblait n'être fixé que dans le dessein de ne pas imposer aux fournisseurs de services de télécommunication une conservation trop longue[981].

1195 Par conséquent, la doctrine était d'avis que la prescription de durée d'une demi-année est une simple prescription d'ordre qui n'empêche pas le fournisseur du service de télécommunication ou d'accès internet à fournir des données sur plus de six mois[982]. Dès lors, les données accessoires de plus de six mois auraient également été exploitables comme moyen probatoire (art. 141 al. 3 CPP).

---

[979] ATF 130 II 249, 254; HEINIGER, n° 11.

[980] MOREILLON, PAREIN-REYMOND, art. 274 N 19; STRÄULI, p. 129.

[981] Message, CPP, p. 1233.

[982] HANSJAKOB, BÜPF/VÜPF, art. 5, n° 21; PERRIER DEPEURSINGE, art. 273, p. 357; StPO-HANSJAKOB, art. 273, n° 14.

1196 Pendant longtemps, le Tribunal fédéral a laissé cette question ouverte indiquant, toutefois, que les infractions commises au moyen d'Internet bénéficient d'une disposition procédure spéciale, comme nous le verrons[983]. Cela étant, le Tribunal fédéral en a décidé autrement, aussi longtemps que le législateur n'aura pas modifié la lettre de la loi. Dans un arrêt récent, notre Haute cour a déclaré que les données secondaires ne pouvaient être ordonnées que pour une durée de six mois, même si le fournisseur a conservé les données plus longtemps en arrière[984].

e) La communication au prévenu et aux tiers sujets de la surveillance

1197 Au plus tard dès la clôture ou la suspension de la procédure préliminaire (art. 318 CPP) correspondant au terme de la mesure de surveillance, le magistrat verse au dossier les résultats ou informations obtenues et avertit les personnes concernées – auteurs présumés et tiers dont le raccordement ou l'accès a été surveillé, ce qui exclut les correspondants de la personne surveillée[985] – qu'elles ont fait l'objet d'une surveillance des télécommunications (art. 279 al. 1 CPP). Le recueil des données accessoires est également soumis à l'obligation de communication.

1198 Cette obligation de communication vise à permettre aux personnes concernées par la surveillance de faire valoir leur droit de recours effectif dont dispose tout être humain impliqué dans une procédure[986] (art. 13 CEDH, art. 14 § 5 Pacte II, art. 32 al. 3 Cst et art. 393 à 397 CPP). C'est pourquoi, le ministère public doit informer lesdites personnes de la forme de la surveillance, des motifs ayant déterminés la surveillance, la méthode technique et la durée de la surveillance (art. 279 al. 1 CPP). A noter que l'exigence de communication ne fait aucune distinction entre les cas où les données résultant de la surveillance sont utilisées comme preuve et ceux où elles ne le sont pas, puisque l'un dans l'autre, il y a eu atteinte au droit individuel (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et 13 al. 1 Cst)[987].

---

983 ATF 139 IV 98,101-102 = JdT 2014 IV 3, 6-7; PERRIER DEPEURSINGE, art. 273, p. 357. Infra Partie II, Chapitre 3, A, III, A, 3, ii, n° 2060.

984 ATF 139 IV 195, 197.

985 HANSJAKOB, BÜPF/VÜPF, art. 10 N 24 et 28; HAUSER, SCHWERI, HARTMANN, p. 361.

986 HANSJAKOB, BÜPF/VÜPF, art. 10 N 10; OBERHOLZER, Strafprozessrechts, p. 429; PERRIER DEPEURSINGE, art. 279, p. 363.

987 ATF 109 Ia 273, 298-303 = JdT 1985 I 616, 618; ATF 123 IV 236, 241 et 244 = JdT 1999 IV 76, 76 et 79; ATF 138 I 6, 33-34.

1199 Nonobstant le devoir de communication au plus tard lors de la clôture de la procédure préliminaire, il est possible de différer l'information sur la surveillance, voire d'y renoncer (art. 279 al. 2 CPP).

1200 En effet, si les informations ne sont pas utilisées comme preuve et que de différer ou de renoncer est utile et indispensable pour préserver un intérêt prépondérant – enquête en cours, maintien de la sécurité publique, lutte contre le crime organisé, etc. –, le tribunal des mesures de contrainte peut accorder sur demande que la communication ne soit pas réalisée au sens de l'alinéa 1er de l'art. 279 CPP.

v. L'exploitation des données recueillies

1201 L'écoute téléphonique et l'interception des communications en général fournissent toute une série d'informations. Elles peuvent être protégées par le secret professionnel, ne présenter aucun rapport avec les faits à élucider, découler d'une surveillance non-autorisée, faire partie de ce qu'on nomme les découvertes fortuites ou être utiles à la découverte de la vérité matérielle. La législation suisse différencie toutes ces catégories de données pouvant être issues de la surveillance des télécommunications. En principe, seules les informations obtenues qui ont trait à l'enquête peuvent être exploitées[988].

a) La protection du secret professionnel

1202 La surveillance des télécommunications doit préserver le secret professionnel (art. 271 al. 1 CPP *cum* 170 à 173 CPP et 321 CP), soit toutes personnes bénéficiant du secret de fonction, du secret professionnel, de la protection des professionnels des médias ou pouvant invoquer un devoir de discrétion[989]. Le régime de surveillance institué par l'art. 271 CP est un régime spécial dès lors que cette catégorie de personnes peut bénéficier du droit de refuser de témoigner.

1203 Dans le dessein d'éviter que le prévenu ne puisse bénéficier de la protection reconnue au détenteur du droit de refuser de témoigner (art. 170 à 173 CPP), les bénéficiaires du secret peuvent faire l'objet d'une surveillance des télécommunications aux mêmes conditions requises pour la surveillance de tout un chacun, et ceci dans quatre hypothèses. La mesure de contrainte est possible: si le prévenu est détenteur du secret professionnel et que des

[988] Message, LSCPT, p. 3719.

[989] EICKER, HUBER, p. 182; GOLDSCHMID, Überwachung, p. 135-150; HANSJAKOB, BÜPF/VÜPF, art. 4 N 18-19; JEANNERET, KÜHN, p. 317; PERRIER, VUILLE, p. 165.

raisons particulières l'exigent (art. 271 al. 2 CPP)[990], si le prévenu se sert de manière active du raccordement téléphonique ou informatique d'un tiers soumis au secret professionnel (art. 270 let. b ch. 1 CPP), si le tiers reçoit des communications déterminées pour le compte du prévenu ou qui émanent du prévenu (art. 270 let. b ch. 2 CPP), ou si une personne sous écoute converse avec un interlocuteur dépositaire du secret, à ce sujet la question de l'exploitabilité des données recueillies doit être analysée de cas par cas après analyse (art. 271 al. 3 CPP).

1204 L'art. 271 al. 2 CPP se réfère à la notion de "branchement direct". Le branchement direct est défini comme "la transmission directe de la correspondance par télécommunication des personnes surveillées entre le service et l'autorité ayant ordonné la surveillance, qui enregistre elle-même ces données" (Annexe ch. 5 de l'art. 2 OSCPT).

1205 Aujourd'hui, malgré le texte de la loi, ce type de branchement est devenu obsolète et est remplacé par la technologie LIS – Lawful Interception System[991]. Cette technologie permet que les informations échangées lors de la correspondance soient enregistrées et mémorisées sur un serveur central du SCPT, et jamais dirigées directement à la police. Néanmoins, il est possible pour l'autorité d'enquête de consulter en ligne et en temps réel les données *via* un accès sécurisé et limité à certaines personnes.

1206 Malgré les avantages de l'application LIS, le tri automatique des données de télécommunication couvertes par le secret professionnel est actuellement impossible. Il apparaît que le service en charge de l'enquête ne devrait pas intercepter en temps réel les données, et que seules les personnes chargées du tri des informations désignées par le droit cantonal doivent avoir accès au LIS (art. 271 al. 1 CPP)[992].

1207 Le tri des communications récoltées s'effectue sous la surveillance d'un magistrat indépendant afin d'éviter qu'un acteur de la procédure pénale puisse avoir connaissance des informations pour lesquelles le droit de refuser de témoigner existe[993]. Il va sans dire que l'autorité judiciaire peut être contrainte d'éliminer immédiatement – c'est-à-dire de ne pas conserver des supports de données, ni des transcriptions – des informations pourtant

990 ATF 106 IV 413, 424-425; ATF 117 Ia 341, 350; ATF 125 I 46, 49-51 = JdT 2000 IV 17, 20-22; ATF 126 II 495, 501-502.

991 AELLEN, HAINARD, n° 14; HANSJAKOB, BÜPF/VÜPF, art. 4 N 66; HANSJAKOB, Zwangsmassnahmen, p. 109; SCHMID, Handbuch, p. 506; SCHMID, Praxiskommentar, art. 271 N 6.

992 AELLEN, HAINARD, n° 4, 7, 14 et 15; CONSEIL FÉDÉRAL, Rapport modification LSCPT, p. 44-45; CR-CPP-BACHER, ZUFFEREY, art. 271 N 11; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 449-451.

993 CourEDH, Affaire *Kopp c. Suisse*, arrêt du 25 mars 1998, 23224/94, § 68-69; EICKER, HUBER, p. 183; STRÄULI, p. 162.

pertinentes, par exemple parce qu'elles ont été interceptées sans rapport avec le motif ou l'objet[994].

1208 En pratique, il est parfois difficile à appréhender par avance si des interlocuteurs sont soumis au secret professionnel, notamment parce que l'identité des interlocuteurs n'est pas connue. Dans l'hypothèse où, en cours de surveillance, l'autorité apprend qu'une cible est tenue au secret, la surveillance est immédiatement stoppée entraînant l'interdiction d'accès au LIS et une procédure de tri doit être instaurée (art. 271 al. 1 CPP). Les informations préalablement récoltées, les supports et les procès-verbaux des conversations sont immédiatement détruits au sens de l'art. 271 al. 3 CPP *cum* les art. 276 al. 1, après la clôture de la procédure, et 277 al. 1 CPP[995]. Cette procédure est cependant vivement critiquée par Laurence Allen et Frédéric Hainard puisqu'elle ne permet plus la pesée des intérêts entre la manifestation de la vérité et l'intérêt au maintien du secret[996].

b) Les informations non-nécessaires à la procédure pénale

1209 Les données recueillies lors d'une mesure de surveillance des télécommunications sont nombreuses impliquant que certaines ne sont pas utiles à élucider l'état de fait[997]. Ce constat démontre l'importance de trier les informations recueillies afin d'écarter celles qui sont sans pertinence pour l'affaire.

1210 Contrairement à ce qui prévaut pour la protection du secret professionnel, la séparation entre les données nécessaires ou celles n'ayant aucune utilité s'effectue souvent en cours de procédure – au moment où il est possible de déterminer l'usage qui peut en être fait – par la police ou le ministère public[998]. Il n'est pas rare que la pertinence ou non des éléments ne puisse est retenue qu'à la fin de la procédure. Dans une telle hypothèse, le tribunal est compétent pour effectuer le tri[999].

1211 Toutes les informations considérées comme non-nécessaires à la procédure pendante sont conservées séparément dans un dossier fantôme inaccessible aux parties (art. 276 al. 1

994 Message, CPP, p. 1231; STRÄULI, p. 163.

995 AELLEN, HAINARD, n° 15; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 452.

996 AELLEN, HAINARD, n° 34

997 GOLDSCHMID, Überwachung, p. 202; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 454; StPO-HANSJAKOB, art. 271 N 15.

998 GOLDSCHMID, Überwachung, p. 130-131; HANSJAKOB, BÜPF/VÜPF, art. 8 N 12 ss; MOREILLON, PAREIN-REYMOND, art. 276 N 3; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 457.

999 GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 266.

CPP)[1000]. Après clôture définitive de la procédure, les informations contenues dans ce dossier ne s'étant pas avérées ultérieurement importantes, elles sont immédiatement détruites (art. 276 al. 1 *in fine* CPP)[1001]. A noter qu'en cas de révision, les documents ne seront alors plus disponibles[1002].

c) Les informations recueillies lors d'une surveillance non-autorisée

1212 Si l'autorisation n'a pas été demandée, si elle n'a pas été accordée, si elle n'est pas prolongée ou si l'autorisation provisoire a été retirée, les résultats de la surveillance non-autorisée sont inexploitables et ce de manière absolue (art. 277 al. 2 CPP)[1003]. Dès lors, les informations recueillies ne sont en aucun cas utilisables comme moyen de preuve (art. 141 al. 1 phr. 2 CPP) et ne peuvent pas servir dans le cadre de l'enquête[1004].

1213 Lorsque l'arrestation d'un prévenu a eu lieu grâce à des données transmises lors d'une surveillance ordonnée mais pas encore autorisée et que, par la suite, l'autorisation n'est pas octroyée, les informations ne sont pas utilisables et donc, vraisemblablement, il faut libérer le prévenu à défaut de soupçons ou de preuves suffisantes.

1214 Dans tous les cas, lorsqu'une autorisation fait défaut, l'autorité judiciaire doit immédiatement détruire tous les documents et supports de données relatifs à ce type de surveillance.

d) Les découvertes fortuites

1215 Quatrième catégorie de données pouvant être interceptées par la surveillance, les découvertes fortuites mettent en lumière un autre acte délictuel commis par le prévenu ou par un tiers (art. 278 al. 1 et 2 CPP)[1005].

[1000] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 235; HANSJAKOB, BÜPF/VÜPF, art. 8 N 19; MÉTILLE, Thèse, p. 204; MOREILLON, PAREIN-REYMOND, art. 276 N 1; STRÄULI, p. 164.

[1001] HANSJAKOB, BÜPF/VÜPF, art. 8 N 21; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 266; STRÄULI, p. 164.

[1002] HANSJAKOB, BÜPF/VÜPF, art. 8 N 21; MOREILLON, PAREIN-REYMOND, art. 276 N 4.

[1003] ATF 131 I 272, 281; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 235; HANSJAKOB, BÜPF/VÜPF, art. 7 N 38; MOREILLON, PAREIN-REYMOND, art. 277 N 2; PERRIER DEPEURSINGE, art. 277, p. 361.

[1004] ATF 131 I 272, 281.

[1005] BIEDERMANN August, p. 91; CR-CPP-BACHER, ZUFFEREY, art. 278 N 1; GOLDSCHMID, Überwachung, p. 202-206; MOREILLON, PAREIN-REYMOND, art. 278 N 3; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 456; SCHMID, RPS, p. 285 et 288.

1216 Le principe de base veut qu'une autorisation soit donnée pour justifier la mise sous surveillance des télécommunications. Ce n'est donc pas parce que le prévenu ou un tiers est licitement surveillé pour une infraction concrète qu'il est possible de prouver d'autres actes délictuels avec les données recueillies[1006]. Qu'il s'agisse d'une autre infraction commise par la personne surveillée (art. 278 al. 1 CPP) ou par un tiers (278 al. 2 CPP), les découvertes fortuites ne sont exploitables que si une surveillance aurait pu être ordonnée même si les soupçons interviennent lors de la surveillance[1007].

1217 Dans le cas de découvertes fortuites, le ministère public ordonne la surveillance avant que la procédure d'enquête ne débute et que les résultats obtenus soient reprochés à la personne mise en cause. Puis, il demande l'autorisation au tribunal des mesures de contrainte qui doit notamment se déterminer sur la possible utilisation des informations obtenues postérieurement (art. 278 al. 3 CPP)[1008].

1218 Toutes les informations fortuites inutiles ou ne remplissant pas les conditions de mise sous surveillance doivent être écartées du dossier et immédiatement détruites après la clôture de la procédure (art. 278 al. 4 CPP), y compris les éléments recueillis grâces aux découvertes fortuites[1009].

1219 Une exception existe néanmoins au principe général de destruction. Les données découvertes fortuitement pouvant permettre de rechercher une personne signalée sont dans toutes les hypothèses utilisables (art. 278 al. 5 CPP).

1220 Ce régime d'exception pourrait laisser penser qu'une mesure de surveillance peut être mise en place sans autorisation si elle a pour but de retrouver une personne[1010]. Même si cette remarque doit être nuancée, puisqu'une surveillance visant à rechercher une personne sans autorisation est illégale et le résultat inexploitable, nous sommes d'avis que cet alinéa n'est pas cohérent avec la procédure de surveillance.

1221 En effet, le régime d'autorisation a été mis en place pour éviter les dérives et protéger le mieux possible les individus pouvant être atteints dans leurs droits personnels et ainsi

---

1006 ATF 141 IV 459, , SJ 2012 I 466, 467-468.

1007 ATF 132 IV 70, 74-75; ATF 140 IV 40, 43-44; ATF 141 IV 459, 460; TF 1B_159/2007 du 23 août 2007, c. 1.2; SJ 2012 I 466, 467-468; HANSJAKOB, forumpoenale, p. 215; JEANNERET, KÜHN, p. 318; MOREILLON, PAREIN-REYMOND, art. 278 N 1 et 4.

1008 GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 267 ss; SCHMID, RPS, p. 299-300.

1009 ATF 133 IV 329, 332-333 = JdT 2009 IV 29, 32-33; ATF 137 I 218, 223-224; ATF 141 IV 459, 460-461; SJ 2012 I 466, 468; MÉTILLE, Thèse, p. 204; SCHMID, RPS, p. 308-310.

1010 SCHMID, RPS, p. 303-304.

respecter le principe de proportionnalité. *In casu*, l'utilisation de l'exception rend exploitables des données non-autorisées alors même que le but et l'objet de la surveillance n'étaient pas la recherche d'une personne déterminée. Il est donc pour le moins surprenant que, dans un tel cas, la proportionnalité et la protection des personnes soient reconnues et que les résultats soient exploitables.

e) Les données exploitables

1222 Outre les données non-exploitables ou non-utilisables, toute une série d'informations sont utilisables, mais pas toujours en l'état.

1223 En général, les communications interceptées sont retranscrites, traduites, voire analysées. En somme, pour respecter le secret professionnel, ne pas divulguer des informations inutiles ou des découvertes fortuites inutilisables, les informations utiles à l'enquête ou exploitables comme moyen probatoire sont séparées des autres données. Le découpage des communications pouvant être erroné ou mener à une incompréhension de l'information recueillie, les données originales sans transformation sont conservées.

1224 Malgré le fait que le CPP ne prévoie pas de destruction pour les informations originelles, il est recommandé de les éliminer immédiatement après l'entrée en force d'une décision judiciaire ou de non-entrée en matière, conformément aux principes jurisprudentielles et aux droits fondamentaux[1011].

1225 Concernant les données accessoires permettant l'identification des usagers (art. 273 al. 1 let. a CPP) et celles relatives à la facturation (art. 273 al. 1 let. b CPP), le Tribunal fédéral a réfuté l'avis de la doctrine concluant qu'elles étaient en tout temps utilisables même si elles datent de plus de six mois lorsque la surveillance est autorisée[1012]. En effet, les données ne peuvent pas dater de plus de six mois ou, à tout le moins, ne peuvent pas être exploitée si elles sont plus anciennes.

d. Les normes élémentaires à la surveillance privée des télécommunications

1226 L'interception des communications par des privés est de plus en plus fréquente grâce aux facilités qu'offre l'évolution technologique. Alors qu'il y a quelques années, il était uniquement

[1011] TF 1C_ 363/2014 du 13 novembre 2014, c. 2 = SJ 2015 I 128, 129-130.

[1012] ATF 139 IV 195, 197. Supra Partie II, Chapitre 3, I, A, 2, c, iv, d), n° 1194.

possible d'enregistrer à l'insu de son interlocuteur la conversation téléphonique ou éventuellement d'utiliser des moyens d'enregistrement pour écouter la conversation entre deux ou plusieurs tiers, il est aujourd'hui possible d'insérer des programmes dans l'ordinateur d'une personne ou dans son téléphone mobile pour dévier ou transférer toutes les données reçues. En outre, il est toujours possible de copier ou de transférer les messages écrits manuellement lorsque le téléphone mobile ou l'ordinateur n'est pas protégé par un mot de passe ou que ce dernier est connu par l'auteur de la prise de données. Néanmoins, ces divers comportements ne sont pas toujours licites.

1227 Contrairement à la surveillance effectuée par les autorités, la surveillance privée – nous entendons par là : l'écoute, la transmission et/ou l'enregistrement des communications même ponctuel – n'est pas régie en tant que telle par la procédure pénale[1013].

1228 Le Code de procédure pénale ne régit que la poursuite et le jugement par les autorités pénales. Les art. 269 ss CPP ne sont donc pas contraignants pour un particulier.

1229 Même si la règle voulait que l'opposabilité ne soit pas reconnue[1014], le Tribunal fédéral reste nuancé à ce sujet. Néanmoins, la Cour a jugé recevable un enregistrement d'une conversation téléphonique conforme à l'art. 179*quinquies* CP alors même que les règles de procédure imposées à l'autorité n'ont pas été respectées par le particulier[1015].

1230 Les informations recueillies lors d'écoutes privées peuvent donc faire office de preuve[1016].

1231 Dans le cadre pénal, le Code pénal protège quelques aspects du droit à l'intimité ou à la vie privée. Les articles spécifiques (art. 179*bis* à 179*septies* CP) favorisent le développement des individus dans leur relation personnelle notamment contre les ingérences de tiers. Ils sont complétés par la protection accordée en droit civil (art. 28 CC et art. 49 CO), ainsi que par d'autres dispositions du Code pénal (art. 186 CP, 173 ss CP, etc.) ou des normes spécifiques à une situation, notamment le droit du travail ou des assurances.

1232 Les comportements typiques que constituent l'écoute et l'enregistrement des conversations – exclusion faite de la lecture d'email ou de SMS qui ne constituent pas des comportements délictueux[1017] – peuvent toutefois être justifiés par les actes autorisés par la loi, la légitime

[1013] GAUTHIER, Enregistrement clandestin, p. 338.

[1014] HAUSER, SCHWERI, HARTMANN, p. 286.

[1015] ATF 114 IV 20 = JdT 1989 IV 8.

[1016] Supra Partie I, Chapitre 3, III, B, 3, e, n° 311.

[1017] Supra Partie II, Chapitre 3, I, A, 2, b, i, n° 1134.

défense ou l'état de nécessité[1018], étant précisé que l'admissibilité des preuves illégales n'est néanmoins pas toujours exclue. Il s'agit alors d'une sorte d'état de nécessité dans le domaine de la preuve, appelé *Beweisnotstand*[1019].

1233 A teneur de sa jurisprudence, le Tribunal fédéral a reconnu qu'il n'y avait pas lieu d'écarter par principe une preuve obtenue par un procédé illicite, notamment l'enregistrement des conversations[1020]. Dans un tel cas de figure, l'acte délictuel ou les propos tenus au sujet d'un tel acte doivent être commis par le prévenu sans aucune influence extérieure, et un moyen licite réalisé par l'autorité aurait dû permettre d'obtenir ces informations[1021]. En outre, il convient de mettre en balance les intérêts de l'Etat à ce que les soupçons soient confirmés ou infirmés et l'intérêt de la personne concernée à voir ses droits personnels sauvegardés[1022], et ceci en fonction de la gravité de l'infraction perpétrée. Il est également admis, notamment par la Cour de justice genevoise et le Tribunal fédéral[1023], que lorsqu'une personne perpètre une infraction au moyen d'un téléphone, un enregistrement illicite peut toujours être utilisé comme preuve.

1234 Par conséquent, les informations recueillies lorsqu'un particulier écoute ou enregistre un ou des tiers sont très largement administrables comme preuves au cours d'un procès pénal.

3. L'usage et le moyen probatoire

a. L'utilisation des informations recueillies

i. En cas de surveillance répressive ou mixte

1235 Le but des mesures de surveillance prévue par le CPP est avant tout de récolter des informations afin de confondre un prévenu et de prouver les suspicions préalables à la mise sous surveillance. Elles peuvent ainsi être utilisées pour prouver des faits passés ou servir à

[1018] HURTADO POZO, art. 179*bis* N 2213; SCHUBARTH, Strafrecht, art. 179 N 39 et art. 179*bis* N 40.

[1019] Supra Partie I, Chapitre 3, III, B, 3, e, n° 311.

[1020] ATF 131 I 272, 278-282; ATF 137 I 218, 223-224 = JdT 2011 I 354, 358-359.

[1021] CR-CPP-BÉNÉDICT, TRECCANI, art. 139-141 N 12; ROTH, p. 71.

[1022] ATF 109 Ia 244, 245-246 = JdT 1984 IV 160 = SJ 1984 I 153; ATF 131 I 272, 278-282; ATF 137 I 218, 223-224 = JdT 2011 I 354, 358-359; CourEDH, Affaire *Schenk c. Suisse*, arrêt du 12 juillet 1988, 10862/84, § 41.

[1023] ATF 109 Ia 244, 246-248 = JdT 1984 IV 160 = SJ 1984 153; SJ 1986 636, 637-638; ATF 138 IV 169, 171.

la poursuite d'infractions en série s'étalant sur une période plus ou moins longue, par exemple pour les trafics de drogue[1024].

1236 En outre, en vertu des normes législatives fédérales et cantonales sur la police, la surveillance à titre préventif n'est pas exclue[1025].

1237 Selon qu'il s'agisse d'une surveillance répressive ou préventive, les normes d'application ne sont donc pas les mêmes.

1238 Aux fins d'exploiter les informations recueillies pour l'enquête ou comme moyen probatoire, il est essentiel de différencier les mesures à but préventif ou de police et celles à dessein répressif ou judiciaire.

1239 En théorie, la distinction entre surveillance répressive ou préventive est relativement aisée, soit elle sert à réprimer un acte délictuel donc à obtenir des indices, voire des preuves, soit elle est utile pour prévenir ou dissuader la commission d'infractions. En pratique, elle peut se confronter à quelques difficultés.

1240 Dans l'hypothèse où l'autorité judicaire porte de forts soupçons sur la commission d'une infraction continue ou que la surveillance s'effectue en lien avec les actes préparatoires d'un acte délictuel non encore commis, la nature de la surveillance est à la fois préventive et répressive[1026]. Dans de telles circonstances, la règle veut qu'à défaut de surveillance purement préventive et lorsqu'il y a suspicion d'actes délictueux, la législation procédurale s'applique et non la loi sur la police[1027].

1241 Ainsi, si la procédure prévue dans le CPP est respectée, les informations obtenues sont exploitables comme preuve.

[1024] Message, CPP, p. 1235; OBERHOLZER, Strafprozessrechts, p. 441-442; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 435-436.

[1025] ATF 134 IV 266, 279-280 = JdT 2008 IV 35, 53.

[1026] Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 436-437.

[1027] Message, CPP, p. 1235.

ii. En cas de surveillance préventive

1242 En cas de surveillance purement préventive, la situation est plus délicate. Actuellement, certains cantons n'ont pas légiféré sur une telle surveillance ou sont en train de le faire. Une telle surveillance dans ces cantons est donc, pour l'heure, illicite[1028].

1243 Par conséquent, si des données de communication sont récoltées à la suite d'une surveillance préventive qui ne peut s'appuyer sur aucune norme de police, les informations obtenues sont inexploitables nonobstant le fait qu'elles peuvent servir à élucider une infraction ou à enclencher une procédure d'enquête.

iii. En cas d'écoute ou d'enregistrement effectué par des particuliers

1244 Quant aux communications écoutées, interceptées et/ou enregistrées par une personne privée, l'atteinte à la personnalité causée par la surveillance à l'insu d'autrui empêche l'utilisation de propos concernant des faits personnels, mais pas les déclarations objectives en lien avec un acte pénalement répréhensible[1029].

1245 Le juge étant libre de former son intime conviction sur tous les éléments administrés, les enregistrements ou les témoignages en lien avec une écoute/interception d'une communication ne sont pas inaptes à servir de preuve. Néanmoins, il est nécessaire que les enregistrements ou les dires soient fidèles à la réalité des événements et ne soient pas modifiés. En cas d'enregistrement, un expert peut donner son opinion quant à une possible transformation et, en cas de témoignage, le faisceau de preuves ne doit pas démontrer que les dires du témoin sont manifestement inexacts ou illogiques.

1246 La jurisprudence a précisé que l'autorité d'instruction et/ou d'enquête peut se servire de ce type de preuve, dans toutes les hypothèses où elle-même aurait pu obtenir légalement ce moyen probatoire[1030], avec la précision que la doctrine retient que la preuve est également exploitable si aucun autre moyen ne permettait de l'obtenir et sous certaines réserves, notamment liées à l'urgence[1031].

[1028] Infra Partie II, Chapitre 3, I, A, 4, c, ii, n° 1355 ss.

[1029] ATF 109 Ia 244, 246-247 = JdT 1984 IV 160 = SJ 1984 153; ATF 133 IV 329, 333 = JdT 2007 IV 29, 32; ATF 138 IV 169, 171; GAUTHIER, Audio-surveillance, p. 83; GAUTHIER, Enregistrement clandestin, p. 338; GODENZI, p. 335 ss.

[1030] TF 6B_983/2013 du 24 février 2014, c. 3.3.1; TF 6B_ 789/2015 du 8 février 2016, c. 3.1; GODENZI, p. 264 et 314.

[1031] GODENZI, p. 264 ss.

b. Les données issues de la surveillance des télécommunications comme moyen de preuve

1247 La surveillance des télécommunications effectuée dans le respect des normes pénales, procédurales et constitutionnelles peut apporter un grand nombre d'informations.

1248 Du point de vue de l'enquête pure, les mesures de surveillance des télécommunications limitent le nombre de policiers mobilisés sur une affaire, économisent des investigations secrètes telles que les filatures et fournissent une preuve – à tout le moins en apparence, suffisamment accablante et difficilement contestable par le prévenu[1032].

1249 Du point de vue juridique, la mesure des techniques de surveillance ayant pour but principal de lutter efficacement et sans lacune contre la criminalité, elle peut prouver la commission de certaines infractions par la personne soupçonnée faisant l'objet de la surveillance ou la commission d'une autre infraction, voire la perpétration de l'infraction par une autre personne lorsque l'autorisation rétroactive est possible – suite à une découverte fortuite – ou pour identifier formellement un auteur individualisable par son raccordement mais pas identifiable sans la mesure de surveillance[1033].

1250 Concernant l'élucidation des faits relatifs à un acte délictuel, les mots, qui sont un support d'informations échangées entre deux ou plusieurs personnes, sont employés comme preuve. C'est donc l'information recueillie elle-même qui est utilisée après traitement – élimination des données relevant du secret professionnel, inutiles ou découlant d'une découverte fortuite qui ne pourrait être utilisée à défaut d'autorisation rétroactive – et est soumise à l'appréciation du juge. Pour permettre la réalisation de cet objectif, la quantité de données recueillies lors de la surveillance ne doit donc pas être trop importante pour permettre leur traitement. C'est pourquoi il est essentiel que les mesures de surveillance soient ciblées.

1251 Concernant les renseignements sur les raccordements et la transmission des données permettant d'identifier les usagers (art. 13 al. 1 let. e, art. 14 al. 1 et 4 et art. 15 al. 5*bis* LSCPT), ils accompagnent généralement la surveillance. Ces informations sont essentielles pour déterminer de manière précise qui est vraisemblablement l'auteur (les auteurs) de l'acte délictuel. Néanmoins, ces renseignements ne doivent pas conduire l'autorité pénale à

[1032] BRODEUR, p. 560; COMMISSION DE RÉFORME DU DROIT DU CANADA, p. 95; CUSSON, Nouvelles technologies, p. 135; GIANNALOPOULOS, PARIZOT, p. 252 ; HUYGHE, La vie numérique.

[1033] BONDALLAZ, protection des personnes, p. 513, 515 et 521; HUYGHE, Ecoutes téléphoniques, p. 32; JOBARD, SCHULZE-ICKING, p. 102.

s'imaginer qu'en tout état de cause les personnes identifiées sont les auteurs. L'enquête et les circonstances de l'affaire doivent appuyer ces constatations.

1252 En définitive, l'acceptation des interceptions de télécommunication en tant que moyen de preuve facilite et accroît la certitude sur l'établissement des faits et l'identité de leur(s) auteur(s).

4. La discussion sur la preuve obtenue à l'aide de la surveillance des télécommunications

1253 La surveillance des communications fournit des informations qui sont sans conteste utilisables comme un moyen de preuve en apparence objectif. Même s'il est exact d'affirmer que les données recueillies revêtent une certaine qualité, il n'en reste pas moins qu'elles sont sujettes à traitement pour être administrées devant l'autorité pénale, et que, par conséquent, elles ne sont pas dénuées de toute subjectivité. Il ne s'agit ainsi pas d'une preuve irréfutable, mais d'un moyen probatoire ayant des forces et des faiblesses.

a. Le potentiel de la surveillance des télécommunications

i. La technicité de la preuve obtenue par le biais de la surveillance

1254 Les interceptions téléphoniques ou de messageries constituant une technique scientifique, la preuve obtenue est par conséquent plus fiable que les preuves classiques telles que le témoignage[1034]. La subjectivité du témoin laisse en effet place à l'objectivité de la technique d'interception et d'enregistrement.

1255 Bien entendu, pour que la surveillance soit réalisée dans le respect du cadre légal et fournisse des informations en quantité suffisante sans rendre le tri des données gargantuesque, il est nécessaire que le SCPT maîtrise la technicité et choisisse la méthode la plus viable dans le cas concret.

1256 Par exemple, pour éviter toute perte de données, si un usager utilise le même téléphone mobile avec diverses cartes SIM, ce n'est pas le numéro IMSI – identifiant la carte SIM, extensivement le titulaire du raccordement – qu'il faut surveiller; il est préférable d'effectuer

[1034] GIANNALOPOULOS, PARIZOT, p. 252. Supra Partie I, Chapitre 3, IV, A, 2, n° 337-340.

la surveillance de l'appareil directement par son numéro IMEI[1035]. De même, en cas d'accès à internet, si l'utilisateur emploie un même compte de messagerie ou plusieurs comptes surveillés, mais se déplace à l'aide d'un ordinateur portable, la surveillance de l'adresse IP occasionne une perte d'informations, alors que la surveillance du compte de messagerie ou de l'adresse MAC de l'ordinateur est plus adéquate.

1257 Quant aux méthodes à disposition, la technique a évolué au point où les compétences pour les mettre en place ou le coût engendré ne sont plus un obstacle. Ainsi, la surveillance des télécommunications, extensivement l'interception des télécommunications, est facilement à la portée de l'Etat. La charge la plus complexe pour obtenir un bon résultat n'est donc pas d'"écouter" les communications, mais de trier et d'analyser les données utiles à l'enquête.

1258 Il n'est plus contesté que la technique est un bienfait pour le travail des enquêteurs et de la justice. Lorsque la méthode est correctement sélectionnée, qu'il existe une collaboration efficace entre l'autorité qui ordonne la surveillance, l'organe qui choisit la méthode et le fournisseur qui l'exécute, il ne fait nul doute que la technicité n'entrave pas la qualité des enregistrements et des informations recueillies. Bien au contraire, grâce aux possibilités d'enregistrement et aux larges éventails de données pouvant être interceptées, la surveillance des télécommunications en tant que mesure objective fournit une certaine force à la preuve.

ii. La difficulté de nier l'évidence d'une information issue de la surveillance

1259 La surveillance peut fournir divers résultats: les données techniques – dates et heures des appels ou messages, numéros ou adresses électroniques des destinataires, durée des communications –, identité – nom, prénom, adresse du titulaire du raccordement–, et le contenu même de la communication.

1260 Hormis les cas où le serveur du fournisseur est victime d'un hacker, il est difficilement concevable de nier la véracité et la certitude des données techniques ou identitaires. Il faut néanmoins garder à l'esprit qu'il n'est pas exclu qu'une entreprise ou une personne soit titulaire de l'abonnement ou de l'accès internet alors même que le raccordement est utilisé par un tiers. Si cette mise en garde reste dans l'esprit des autorités officielles et qu'au besoin la problématique de l'identité de l'usager du raccordement est éclaircie, il est hautement vraisemblable que toutes les données ou informations issues de la surveillance des télécommunications sont correctes. Une durée d'appel ou l'identité du titulaire d'un raccordement n'est en effet pas sujet à interprétation.

[1035] METILLE, Thèse, p. 87.

1261 En outre, l'usage le plus répandu de l'interception des télécommunications concerne le contenu de la conversation. Grâce à la surveillance, ce qu'une personne confie à un ou plusieurs individu(s) est connu des enquêteurs et de la justice. En cas d'élucidation d'une infraction, l'accusé peut difficilement nier les aveux enregistrés à son insu[1036].

1262 En pareille circonstance, la preuve obtenue est assortie d'une force probante importante, ce d'autant plus que, l'aveu ayant été fait hors du commissariat, l'accusé pourra difficilement arguer qu'il est issu de pression ou de menace policière.

1263 L'objectivité des données techniques et identitaires, ainsi que l'importance d'un aveu téléphonique ou écrit apporte une force probante certaine à la preuve issue de la surveillance des télécommunications. En effet, tout élément dénué de subjectivité est largement apprécié par la Cour, ce d'autant si les dires proviennent directement du coupable[1037].

iii. L'efficacité des moyens de surveillance

1264 Les défenseurs de la surveillance exagèrent bien souvent l'efficacité de la surveillance, tout comme les détracteurs exagèrent la méfiance devant être portée à cette technique. Pour certains, la surveillance des télécommunications accroît clairement la sécurité publique, voire fournit l'illusion d'une sécurité totale, alors que pour d'autres, la surveillance est un moyen technique à craindre car trop intrusif dans la vie privée. Il n'en reste pas moins que les interceptions des conversations écrites ou orales sont des moyens de preuves efficaces.

1265 Le fait que nous laissons quotidiennement de plus en plus de traces de nos vies sociales, que ces données peuvent être reliées, conservées et traitées, et que le téléphone mobile ou internet favorise les échanges sont des arguments pro-surveillance. Non seulement les écoutes et enregistrements peuvent permettre d'élucider des infractions, mais le "profilage" créé par l'analyse des échanges offre l'opportunité d'identifier des suspects.

1266 L'autorité d'enquête ou de poursuite ne remet pas (ou rarement) en question les informations recueillies et leur pertinence dans les affaires en cause, et ceci parce que ces deux autorités ont la volonté d'accélérer et de faciliter les recherches du ou des suspect(s)[1038]. Quant à la justice, elle apprécie particulièrement le recours à cette technologie. Elle ne réfute

[1036] HUYGHE, Ecoutes téléphoniques, p. 40 et 57.

[1037] Supra Partie I, Chapitre 3, IV, A, 1, n° 328-331.

[1038] GIANNALOPOULOS, PARIZOT, p. 256.

généralement pas l'objectivité de la preuve apportée et se borne uniquement à signaler que seul l'emploi de la mesure doit être surveillé et contrôlé.

1267 En tout état de cause, personne ne nie l'importance de l'usage de la surveillance dans le dessein de faciliter les investigations et d'obtenir un moyen probatoire objectif, ce d'autant que son objectivité ne se présente pas sous forme de probabilités ou de statistiques, mais de mots provenant des personnes impliquées directement ou indirectement.

1268 *A priori*, ce mode probatoire est donc privé de toute subjectivité liée à une interprétation permettant aisément la recherche de la vérité matérielle par les juges.

1269 Par conséquent, la preuve obtenue par la surveillance des télécommunications traduit incontestablement deux volontés: celle d'accélérer et de faciliter la recherche de preuve, et celle d'établir la vérité matérielle permettant l'accomplissement de deux objectifs de la procédure pénale: la célérité et la recherche de la vérité. Grâce à l'intrusion dans la vie privée des individus, ce moyen de contrainte facilite l'établissement des faits particulièrement ardus à démontrer sans son usage. Une surveillance des communications bien conçue et ciblée contribue rapidement et de manière plus sûre à l'accusation du ou des suspects, puis à leur condamnation[1039] ou, au contraire, à l'(les) innocenter.

b. Les problématiques liées à l'exploitation et à l'administration des informations issues de la surveillance des télécommunications

i. La surveillance incomplète

1270 Le Tribunal fédéral a déclaré que le but principal de la surveillance des télécommunications à des fins pénales est de garantir la lutte efficace et sans lacune contre la criminalité[1040]. En pratique, ni la LSCPT ni le respect des droits fondamentaux ne permettent une telle lutte.

1271 En premier lieu, la liste exhaustive des infractions poursuivies pouvant faire l'objet d'une surveillance rend impossible la poursuite des infractions n'y figurant pas alors même que le comportement pénalement répréhensible est directement lié aux télécommunications[1041]. Par exemple, l'accès indu à un système informatique (art. 143*bis* CP) ne peut pas faire l'objet

[1039] CUSSON, Nouvelles technologies, p. 138; GIANNALOPOULOS, PARIZOT, p. 252 et 256.

[1040] ATF 109 Ia 273, 287 et 291-292 = JdT 1985 I 616, 617.

[1041] BONDALLAZ, protection des personnes, p. 521; StPO-HANSJAKOB, art. 269 N 28.

d'une surveillance (art. 269 al. 2 let. a *a contrario* CPP) quand bien même la surveillance numérique est un moyen adéquat pour identifier l'auteur de l'accès indu.

1272 En second lieu, en vertu de la LSCPT, seuls les fournisseurs de services de télécommunication ou d'accès à Internet doivent collaborer à la surveillance des télécommunications.

1273 Or, si un suspect communique par le biais d'un ordinateur se trouvant dans un cybercafé ou emploie le réseau téléphonique ou internet d'une entreprise, la surveillance n'est alors qu'indirecte dans l'hypothèse où le trafic transite par un opérateur, ce qui a pour effet une possible perte de données et contenus des communications utiles pour élucider l'enquête.

1274 De même, un auteur qui change régulièrement de numéro, de carte SIM, de téléphone, d'ordinateur, d'adresse IP, etc. peut difficilement être surveillé sans encombre et sans perte d'informations.

1275 En troisième lieu, le contenu des conversations pour ce qui est de la surveillance en temps réel est éphémère. Une communication qui n'a pas été enregistrée ne peut être conservée. De même, un email qui n'est pas intercepté avant sa transmission au destinataire ne peut plus faire l'objet d'une surveillance[1042]. Là encore, certaines données nécessaires à l'enquête peuvent être absentes du dossier de surveillance.

1276 Ces constats nous amènent à deux conclusions.

1277 Premièrement, la surveillance des télécommunications n'est pas efficace dans certains cas. En effet, lorsqu'une surveillance ne peut pas se faire – par exemple parce que l'auteur change trop souvent de numéro sans que l'autorité appréhende ce fait, n'a pas d'abonnement à son nom, etc. –, la méthode de surveillance n'est pas viable. Lorsque la surveillance ne peut se réaliser que partiellement – par exemple, parce qu'un seul numéro est surveillé –, il ne fait aucun doute que des données sont perdues alors même qu'elles peuvent être essentielles.

1278 Deuxièmement, il n'est pas impossible ni rare que des informations manquent au dossier – par exemple, suite à un problème technique – rendant imprécises, voire lacunaires les communications interceptées.

[1042] Infra Partie 2, Chapitre 3, III, A, 3, c, iii, n° 2059 ss.

1279 Dans ces deux circonstances, le résultat de la surveillance est alors plus ou moins approximatif apportant des doutes, des incohérences ou des incompréhensions qui peuvent influencer la valeur probatoire de la preuve liée à la surveillance des télécommunications.

ii. La séparation des données utiles et inutiles à la procédure pénale en cours

1280 Nous l'avons préalablement exposé[1043], les données couvertes par le secret professionnel et celles inutiles à la procédure doivent être écartées. La surveillance des télécommunications occasionne donc le tri d'un certain nombre d'informations récoltées.

a) Le problème du dossier fantôme contenant les données issues de la surveillance et écartées du dossier de procédure

1281 Afin de préserver les droits de la défense et permettre la recherche de la vérité, il est essentiel que seules les données totalement inutiles ou liées au secret professionnel soient écartées. En effet, si une donnée utile est ôtée, la conséquence peut être une appréciation erronée de l'état de fait et une condamnation ou un non-lieu injustifié.

1282 Même s'il est vrai qu'une donnée écartée n'est pas totalement effacée puisqu'elle est conservée dans le dossier fantôme qui comprend la totalité des données recueillies et écartées du dossier de procédure, ce dossier n'est pas utilisable directement au procès. Dès lors, si une personne chargée de trier les informations réalise une interprétation erronée, des disfonctionnements de la procédure ne sont pas exclus.

1283 En effet, le juge ne se réfère aux données écartées qu'en cas de doute suffisant sur leur utilité pour l'affaire à juger. Sans savoir ce que comporte le dossier fantôme, il paraît cependant impossible ou très difficile de se déterminer sur l'importance d'une information inconnue parce qu'écartée.

1284 A ce premier constat s'ajoute le fait que certaines informations recueillies peuvent n'avoir aucune utilité en début de procédure et s'avérer, par la suite, indispensables. A nouveau, sauf si le juge, la défense, voire l'accusation se plonge dans le dossier fantôme, certaines informations nécessaires à l'affaire risquent de ne pas apparaître lors du procès, et, par conséquent, ne serviront pas à la recherche la vérité et à la formation de l'intime conviction du juge.

[1043] Supra Partie II, Chapitre 3, A, 2, c, v, a), n° 1202 ss.

1285 Lorsque le juge doit déterminer la valeur probatoire des informations issues de la surveillance des télécommunications – principalement le contenu des communications, il ne doit pas perdre de vue qu'il s'agit de retranscriptions, de résumés ou de données analysées.

b) La modification possible des données recueillies

1286 La garantie de la véracité et/ou de l'authenticité des données n'est possible que si la personne, le fournisseur du service de télécommunication ou d'accès internet employé ou tout autre acteur maîtrise l'information.

1287 Ainsi, les fournisseurs de téléphonie peuvent assurer la titularité officielle du numéro de téléphone et ceci uniquement dans l'hypothèse où le titulaire n'a pas utilisé l'identité d'une autre personne[1044].

1288 En revanche, il n'est pas possible d'assurer notamment que le numéro IMEI, le numéro SIM, l'adresse IP, l'adresse MAC surveillé(e) appartienne bien au suspect, ni même que la surveillance puisse fournir réellement des informations quant aux communications émises.

1289 Une courte recherche sur internet nous permet de faire un constat simple. En tapant "modification numéro IMEI", "changement adresse MAC", "piratage adresse IP" en français et/ou en anglais, voire dans bien d'autres langues, des milliers de résultats apparaissent dont certains renvoient à des sites qui expliquent comment modifier tous ces numéros.

1290 En outre, les hackeurs sont particulièrement doués pour envoyer des emails en utilisant l'adresse mail d'un tiers.

1291 Ainsi, la surveillance peut ne pas fournir la totalité des informations utiles à la procédure, notamment si un numéro spécifique est surveillé et que le suspect le modifie pour échanger des communications.

1292 Personne ne peut en principe assurer que toutes les informations sont bien apportées aux procès, tout comme personne ne peut affirmer qu'elles sont vraies et authentiques, soit non-modifiées. Le juge doit ainsi prendre en considération ce fait pour apprécier la preuve qui lui est apportée.

[1044] BERGIER, CARTIER, RICPTS 2007, p. 483-484; BERGIER, CARTIER, RICPTS 2008, p. 108.

iii. La traduction et l'interprétation des communications échangées

1293 Aujourd'hui, les criminels ne doutent plus des facilités, pour les autorités policière et judiciaire, de mettre en œuvre la surveillance des télécommunications. C'est pourquoi, il est fréquent que les communications soient réalisées en langue étrangère ou qu'elles soient de moins en moins intéressantes dans leur contenu, par exemple parce que les personnes qui communiquent emploient des mots dits codés ou encore, parce que le message électronique est crypté.

a) La traduction des communications

1294 Environ 6'000[1045], c'est le nombre de langues – dialectes compris – que les ethnologues recensent dans le monde. Cette large palette apporte une évidence: il n'est pas exclu qu'un ou des criminels emploient une langue différente que celle des enquêteurs ou de la justice. Dès lors, en cas d'interception d'une communication orale ou écrite en langue étrangère ou nationale autre que celle connue par les différents acteurs de la surveillance, un traducteur doit œuvrer.

1295 La traduction d'un texte ou d'une communication n'est pas aisée et n'est pas l'exacte réalité des dires. Comme le rappelle Pierre Leyris, traducteur: "*Traduire c'est avoir l'honnêteté de s'en tenir à une imperfection allusive*"[1046].

1296 En somme, la traduction d'une communication dans une langue source implique de l'interpréter pour fournir une équivalence dans la langue cible afin de rendre le contenu compréhensible.

1297 En outre, pour permettre une traduction correcte, il est impératif que l'interprète connaisse le vocabulaire ou les expressions liés au domaine concerné.

1298 Par conséquent, la traduction, même la plus fidèle, ne peut pas retranscrire mot pour mot la conversation, ce d'autant que certains mots ou expressions de la langue source ne trouvent pas d'équivalence dans la langue cible. Le facteur d'interprétation et les connaissances lexicales du traducteur ne doivent pas être négligés lorsque le juge cherche à déterminer la valeur probatoire.

[1045] Information disponible sur le site internet de l'UNESCO: http://www.unesco.org [consulté le 08.05.2016].

[1046] Le Monde, *Interview de Pierre Leyris*, article du 12 juillet 1974.

1299 Par ailleurs, le Tribunal fédéral a considéré que la retranscription des écoutes téléphoniques effectuées doit mentionner le nom du traducteur et l'indication que ce dernier a été rendu attentif aux conséquences d'une fausse traduction en justice au sens de l'art. 307 CP[1047]. En l'absence de ces indications, la preuve obtenue au moyen des écoutes téléphoniques, plus précisément de leur traduction, viole le droit d'être entendu, ce qui ne rend pas le moyen probatoire inexploitable, mais implique qu'une traduction conforme aux principes exposés soit réalisée[1048].

b) L'emploi de langage codé par les personnes surveillées

1300 Se référer à la discussion orale ou écrite des participants peut amener des incompréhensions surtout lorsque des codes sont employés.

1301 Même s'il est vrai que "pneu", "pain" et "tapis" sont connus des autorités d'enquête et d'investigation comme signifiant livre ou demi-kilo de cocaïne ou d'héroïne, l'imagination des auteurs d'actes délictuels est infinie[1049]. Il n'est par conséquent pas toujours possible de déterminer avec exactitude la signification d'un code.

1302 Des erreurs d'interprétation ne sont pas impossibles. Pour pallier ce déficit, il est essentiel que le juge s'intéresse au décodage des mots, qu'il ne perde pas de vue que l'interprétation fournie n'est qu'une hypothèse de traduction et qu'il doit déterminer comment cette interprétation a été réalisée et pourquoi un tel résultat, plutôt qu'un autre, est obtenu.

1303 En somme, la justice se doit de ne pas affirmer que le contenu des communications est réel et authentique sans autre mesure. Le magistrat en charge du dossier doit se rappeler que ce qui lui est exposé n'est qu'une proposition ou recommandation et donc que des lacunes ou des irrégularités sont possibles.

[1047] TF 6B_80/2012 du 14 août 2012, c. 1.3 = SJ 2013 I 186, 186-187.

[1048] TF 6B_80/2012 du 14 août 2012, c. 1.4 = SJ 2013 I 186, 187.

[1049] CORNU, p. 247; RUCKSTUHL, p. 152.

c. Quelques pistes de réflexion

i. La surveillance des communications VoIP

a) La technologie VoIP et les chevaux de Troie

1304 La technologie VoIP – *Voice over Internet Protocol* – est utilisée pour communiquer par la voix – similairement à la téléphonie fixe ou mobile – en recourant au protocole TCP/IP[1050]. Ce type de téléphonie a la particularité de pouvoir exister *via* le réseau internet, filaire ou non, ou sur d'autres réseaux compatibles IP, soit les réseaux privés.

1305 L'utilisation de la technologie VoIP pour communiquer pose deux difficultés quant à sa surveillance. Premièrement, il s'agit d'une téléphonie "sans connexion", c'est-à-dire que le protocole TCP/IP ne prédétermine par un chemin pour permettre un échange, contrairement à la téléphonie traditionnelle qui n'est ouverte que lorsque le destinataire a décroché[1051]. Deuxièmement, les communications VoIP sont bien souvent cryptées et donc inutilisables en l'état[1052]. Pour surveiller secrètement les communications utilisant le protocole TCP/IP, la technique de surveillance classique n'est dès lors pas adéquate. L'unique solution est d'installer un logiciel espion dans l'ordinateur ou le Smartphone qui permet d'intercepter la communication à sa source avant tout cryptage[1053].

1306 Grâce à la technique dite du cheval de Troie, il est possible d'introduire à distance un logiciel dans l'ordinateur ou le Smartphone d'un utilisateur. Pour se faire, il suffit notamment d'envoyer un message électronique contenant une pièce jointe avec une dénomination suffisamment intéressante pour que l'utilisateur l'ouvre et que le programme s'installe automatiquement sur l'ordinateur, ou d'introduire le logiciel avec l'aide du fournisseur d'accès ou d'un fabriquant dans une mise à jour de programme. Il est ainsi possible de capturer les échanges de flux entre l'appareil et le réseau dans leur entier ou seulement les échanges liés à certains services spécifiques, voire de surveiller les entrées clavier, soit par exemple les mots de passe tapés.

[1050] BIEDERMANN August, p. 106; BONDALLAZ, protection des personnes, p. 511; JEAN-RICHARD-DIT-BRESSEL, BÜPF, p. 44; PIQUEREZ, Traité de procédure pénale suisse, p. 616-617; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 443.

[1051] BONDALLAZ, protection des personnes, p. 511.

[1052] HANSJAKOB, GovWare, n° 6-7; JAGGI, p. 277.

[1053] HANSJAKOB, GovWare, n° 9; JOTTERAND, MÜLLER, TRECCANI, n° 5.

b) Les normes actuelles sont-elles suffisantes pour autoriser l'utilisation des logiciels espions?

1307 L'art. 15 al. 1 LSCPT permet d'exiger la surveillance des communications *via* le réseau Internet, et la OSCPT réglemente explicitement la question (art. 24 al. 2 let. b OSCPT). Les médias numériques, tels que la technologie VoIP, peuvent donc faire l'objet d'une surveillance des télécommunications.

1308 Néanmoins, un problème subsiste quant à la mise en œuvre d'une telle surveillance *via* le réseau IP. En effet, à ce jour aucune réponse définitive n'est donnée quant à savoir si le CPP permet ou non l'installation d'un logiciel espion, mais cette problématique sera réglée si le référendum de la nouvelle LSCPT n'aboutit pas et/ou si le législateur se détermine positivement sur l'introduction des nouveaux articles du CPP (art. 269*bis* CPP).

1309 A teneur de l'art. 280 let. a CPP, le ministère public peut utiliser des dispositifs techniques de surveillance aux fins d'écouter ou d'enregistrer des conversations non publiques.

1310 La disposition légale et le message du Conseil fédéral ne définissent pas ce qu'il faut entendre par "*dispositifs techniques*"[1054].

1311 Le Tribunal fédéral, dans un arrêt récent, a élargi la notion de "*dispositifs techniques*". Par ces termes, il faut entendre tout moyen utilisé dans un cas concret qui permet d'écouter une conversation non publique[1055]. Cette interprétation large de la norme inclut donc l'emploi de logiciel espion. En effet, même si un cheval de Troie est un programme, il est installé sur un ordinateur, soit un appareil, ce qui est suffisant au regard de l'interprétation du Tribunal fédéral puisque le texte légal ne stipule pas que l'appareil doit appartenir à l'autorité[1056].

1312 A notre sens, l'avis du Tribunal fédéral est erroné tant au regard de l'interprétation littérale, historique, systématique que théologique de la norme[1057].

1313 Littéralement, le libellé de l'art. 280 CP est clair et parle de dispositif technique de surveillance. Thomas Hansjakob[1058] précise que l'art. 280 let. a CPP se réfère à l'utilisation d'appareils d'écoute et d'enregistrement évoqués aux art. 179*bis* et 179*quater* CP. Nous sommes du même avis.

[1054] Message, CPP, p. 1234

[1055] ATF 133 IV 249, 253-254 = JdT 2009 IV 10, 14-15.

[1056] JOTTERAND, MÜLLER, TRECCANI, n° 15.

[1057] Dans le même sens: RISS, ZANON, n° 14-26.

[1058] HANSJAKOB, GovWare, n° 17-18. *A contrario* JOTTERAND, MÜLLER, TRECCANI, n° 15.

1314 Les logiciels de type Govware ne sont en aucun cas des appareils et ne permettent pas l'écoute de la communication, mais uniquement le traitement des données ou l'espionnage des fichiers. Un tel programme permet d'intercepter non seulement les communications orales ou écrites, mais aussi tout type de fichiers contenus dans l'ordinateur allant donc plus loin que l'usage d'un dispositif technique classique. Ainsi, même si nous acceptions la notion large de "dispositifs techniques" réalisée par le Tribunal fédéral, il n'en reste pas moins que l'interception par un cheval de Troie ne se limite pas qu'à l'écoute et à l'enregistrement des conversations[1059].

1315 Historiquement, l'art. 280 let. a CPP a été édicté pour servir de justification aux articles 179*bis* et 179*quater* CP. En revanche, les travaux parlementaires lors de la création de cet article ne font aucune référence à l'utilisation de chevaux de Troie.

1316 En outre, toujours selon l'interprétation historique, ou plus exactement selon une interprétation temporelle, le Tribunal fédéral a reconnu que, pour cette règle d'interprétation, il était acceptable de s'intéresser aux travaux préparatoires sur les projets de loi non-entrés en vigueur[1060]. Les changements de circonstances peuvent permettre de révéler des lacunes dans la loi et être utiles pour interpréter une norme.

1317 *In casu*, la révision de la LSCPT, en procédure de navette entre le Conseil national et le Conseil des Etats, est en cours avec pour point d'orgue l'introduction d'un nouvel article dans le Code de procédure pénale prévoyant spécifiquement l'introduction de logiciel espion pour une surveillance secrète. Ce constat nous conforte dans l'idée que le législateur n'a, lors de l'édiction de l'art. 280 CPP, pas prévu le cas de l'installation de programmes informatiques à des fins de surveillance.

1318 Selon l'interprétation systématique, il faut se référer à la cohérence et l'harmonie de l'ordre juridique. Les mesures de surveillance font partie des mesures de contrainte (Chapitre 8 du Titre 5 du Code de procédure pénale). A teneur de l'art. 196 CPP, la surveillance des télécommunications porte donc atteinte aux droits fondamentaux. Selon la jurisprudence, la sécurité juridique commande que la détermination de la norme et sa prévisibilité dépendent étroitement de la complexité de la mesure, voire de la gravité de l'atteinte.

1319 Lors de l'installation d'un cheval de Troie, l'autorité s'infiltre dans un ordinateur ou un Smartphone à l'insu de l'utilisateur. Il ne fait aucun doute que l'atteinte à la vie privée est

[1059] HANSJAKOB, GovWare, n° 21; Message, P-LSCPT, p. 2468.

[1060] ATF 124 II 193, 201; ATF 131 II 13, 31-32.

grave[1061]. En outre, les chevaux de Troie sont des programmes spécifiques et relativement complexes dont la portée et le fonctionnement sont inconnus de nombreuses personnes pouvant occasionner une grande méfiance. C'est pourquoi l'édiction de normes claires réglant les circonstances et les conditions dans lesquelles un logiciel espion peut être utilisé est nécessaire afin de garantir la prévisibilité.

1320 Enfin, dans la perspective téléologique, il faut se demander si la volonté du législateur était d'admettre que l'art. 280 let. a CPP constitue une norme suffisante pour les chevaux de Troie. L'analogie dans le contexte de l'interprétation des lois n'est pas interdite[1062]. Nous pouvons donc nous demander si tel pourrait être le cas pour admettre l'utilisation des chevaux de Troie. Néanmoins, pour deux raisons, nous rejetons l'application analogique de l'art. 280 let. a CPP pour les logiciels de surveillance.

1321 Premièrement, lors de l'adoption de l'art. 280 CPP, il existait déjà des logiciels d'espionnage et, pourtant, le législateur n'a fait aucune référence à ces programmes lors de l'édiction de la norme[1063]. Il apparaît donc par conséquent qu'il n'a pas voulu autoriser l'utilisation de ce type de surveillance.

1322 Deuxièmement, Thomas Hansjakob relève que le comportement visant à introduire un programme informatique dans un ordinateur est constitutif d'une infraction à l'art. 143*bis* CP[1064]. L'intrusion informatique est en effet réalisée "*sans droit*"[1065]. La mesure étant secrète la question de l'intervention de l'assentiment de l'ayant-droit n'intervient pas pour exclure la typicité, et le législateur a introduit l'art. 280 CPP pour justifier les infractions prévues aux art. 179*bis*, 179*quater* et 179*octies* CP CP, et non celle de l'art. 143*bis* CP. Dès lors, il n'a pas été désireux de prévoir la surveillance aux moyens de logiciels espions.

1323 Par conséquent, à notre avis, l'art. 280 let. a CPP ne nous semble pas suffisant pour admettre ni l'introduction d'un cheval de Troie, ni la possibilité d'utiliser les données VoIP hors transmission externe, et ne respecte vraisemblablement pas la prévisibilité commandée par les droits fondamentaux[1066].

[1061] HANSJAKOB, GovWare, n° 19; Message, P-LSCPT, p. 2389 et 2472; RISS, ZANON, n° 20.

[1062] ATF 87 IV 115, 118-120; ATF 95 IV 68, 72-73; ATF 127 IV 198, 200.

[1063] RISS, ZANON, n° 22.

[1064] CONSEIL FÉDÉRAL, Rapport modification LSCPT, p. 41; HANSJAKOB, GovWare, n° 16 et 18.

[1065] *A contrario*: JOTTERAND, MÜLLER, TRECCANI, n° 18; METILLE, Jusletter, n° 37.

[1066] Dans ce sens: HANSJAKOB, art. 269ter StPO; HANSJAKOB, GovWare; RISS, ZANON. *A contrario*: JOTTERAND, MÜLLER, TRECCANI; METILLE, Jusletter.

1324 Relevons encore que Sylvain Métille, Olivier Jotterand, Jérémie Müller et Jean Treccani différencient l'emploi de chevaux de Troie pour l'interception du flux d'informations échangées ou pour la surveillance de l'environnement informatique. Dans le premier cas, notamment pour la surveillance VoIP, ces auteurs estiment qu'il s'agit d'une simple surveillance de la correspondance au sens de l'art. 269 ss CPP. Dans le second cas, il s'agit d'un dispositif technique de surveillance prévu à l'art. 280 CPP.

1325 Nous réfutons cette distinction puisqu'il ne s'agit pas de surveiller un raccordement ou une communication mais un flux de données.

1326 Dans un arrêt récent, la Cour constitutionnelle allemande a considéré que l'introduction d'un cheval de Troie n'était pas une simple mesure de surveillance des télécommunications, mais ressemblait davantage à une "perquisition en ligne"[1067]. Par conséquent, il s'agit d'une mesure nettement plus invasive que ce que permet l'art. 269 ss CPP qui ne peut pas non plus se justifier au regard de l'art. 245 CPP sur l'exécution d'une perquisition puisque la surveillance est réalisée à l'insu de l'utilisateur.

1327 Dans tous les cas, une base légale spécifique semble nécessaire pour autoriser l'utilisation de chevaux de Troie.

c) La révision de la LSCPT et l'introduction de l'art. 269ter CPP

1328 La révision de la LSCPT prévoit l'introduction d'un article 269*ter* CPP autorisant l'introduction de logiciel d'espionnage et de décryptage des données, ainsi qu'une précision et un complément concernant les personnes soumises à la LSCPT[1068].

1. Le projet de modification de la LSCPT en quelques mots

1329 Le P-LSCPT précise et complète le champ d'application matériel (art. 1 P-LSCPT) et personnel (art. 2 P-LSCPT) pour tenir compte de l'évolution technologique et de l'usage grandissant des télécommunications par Internet.

[1067] BGH StB18/06 vom 31.1.2007, § 5 et 7; BVerfG, 1 BvR 370/07 vom 27.2.2008, § 11.

[1068] CONSEIL FEDERAL, Rapport modification LSCPT, p. 41; FF 2016 p. 1821; HANSJAKOB, art. 269ter StPO, n° 5; HANSJAKOB, Jusletter-IT, n°2; Message, P-LSCPT, p. 2466.

1330 L'art. 2 al. 1 P-LSCPT ne se limite plus à soumettre les fournisseurs d'accès Internet à l'exécution de la surveillance. Les intermédiaires ou les personnes mettant à disposition une infrastructure de communication sont également concernés. Ainsi, les fournisseurs d'hébergement – Service-provider ou Hosting-provider, soit les fournisseurs d'application en ligne – ni soumis à concession, ni à l'obligation d'annoncer sont tenus d'exécuter la surveillance. Cette modification évite ainsi que certains se retranchent derrière la notion "*fournisseur d'accès Internet*" pour refuser la mise en œuvre de la surveillance, notamment VoIP, lorsque la communication ne fait qu'utiliser le réseau sans qu'il y ait d'accès.

1331 Le P-LSCPT est actuellement en examen auprès du parlement. Suite à la session d'automne 2015, les délibérations du Conseil national ont soulevé des divergences, si bien que le P-LSCPT a été renvoyé au Conseil des Etats.

2. La création de l'art. 269*ter* CPP

1332 La surveillance à l'aide d'un logiciel espion, communément appelé GovWare, nécessitant de pénétrer activement dans le système informatique de la personne surveillée est nettement plus invasive qu'un simple détournement des données ou du recueillement de celles stockées. La sphère privée dans sa perspective de droit au secret des télécommunications et à la protection du domicile électronique est mise à mal.

1333 La protection du domicile électronique est le droit le plus touché par l'utilisation des chevaux de Troie[1069]. Il vise à garantir la confidentialité et l'intégrité des informations stockées par les usagers ou les tiers à leur intention dans un espace numérique[1070]. Ce sont ces mêmes informations qui sont interceptées par l'utilisation de logiciels espions ou d'autres dispositifs analogues. Ce droit à la protection du domicile électronique ne fait néanmoins par partie du catalogue des droits fondamentaux institués dans la Constitution. Afin d'assurer la sauvegarde des droit fondamentaux et malgré que le droit au domicile électronique trouve son fondement à l'art. 28 al. 1 CC, il serait préférable que l'art. 13 al. 1 Cst explicite ce droit.

1334 Relevons encore que, comme la déclaré la Cour constitutionnelle allemande[1071], le comportement visant à introduire un cheval de Troie pour surveiller un ordinateur ou un Smartphone constitue une grave atteinte aux droits fondamentaux de la confidentialité, de l'intégrité des données et de la sphère privée. Ce type de surveillance ne peut se justifier que

[1069] BVerfG, 1 BvR 370/07 vom 27.2.2008, § 166.

[1070] BONDALLAZ, Jusletter, n° 61.

[1071] BVerfG, 1 BvR 370/07 vom 27.2.2008, § 245.

si le recours à cette méthode est prévu par une base légale suffisamment claire et prévisible, respecte la proportionnalité et est strictement nécessaire.

1335 Comme nous l'avons vu[1072], à la lumière de la législation en vigueur, la surveillance effectuée par l'introduction d'un cheval de Troie est illicite, malgré qu'à de rare reprise un logiciel GovWare a été utilisé par les autorités policière ou judiciaire avant l'entrée en vigueur, conformément aux dispositions de droit cantonal ou fédéral en vigueur[1073]. C'est pourquoi la modification de la LSCPT ajoute un art. 269*ter* CPP aux mesures de surveillance secrète. Cet article sert non seulement de base légale justifiant l'atteinte à l'art. 143*bis* CP, mais fixe également le cadre de mise en œuvre de la surveillance à l'aide d'un logiciel espion[1074].

1336 L'art. 269*ter* CPP offre une base légale expresse et précise pour recourir aux logiciels d'espionnage, soit des programmes informatiques infiltrés dans le but d'intercepter et de permettre la lecture des données à l'insu de la personne surveillée. Plus spécifiquement, grâce au programme informatique, l'autorité pénale peut surveiller un ordinateur ou un Smartphone et avoir accès à toutes les informations échangées sans qu'elles soient cryptées, permettant notamment de surveiller la téléphonie par Internet et la correspondance par e-mails[1075]. Néanmoins, la disposition légale interdit l'usage d'un logiciel Govware pour perquisitionner en ligne un ordinateur ou tout autre système informatique (téléphone mobile ou fixe, tablette, etc.) ainsi que pour utiliser la caméra ou le micro intégré[1076]. En outre, dans l'hypothèse où un antivirus bloque le programme de surveillance, cette disposition légale permet de mettre en place, pour déjouer le blocage, un second logiciel complémentaire[1077].

1337 Conformément aux obligations légales, le ministère public doit en premier lieu spécifier le type d'informations pouvant être interceptées[1078]. Cette condition fixe une limite dans l'obtention des données issues de la surveillance et doit permettre d'éviter les abus. Néanmoins, l'introduction d'un logiciel informatisé permet d'obtenir non seulement des données précises et utiles à la procédure, et toutes les données stockées sur l'ordinateur même sans rapport avec la procédure de surveillance. Ainsi, la limite légale reste franchissable par l'autorité chargée de la mesure même si les données recueillies ne sont alors pas exploitables (art. 277 CPP)[1079].

[1072] Supra Partie II, Chapitre 3, I, A, 4, c, i, b), n° 1307 ss.

[1073] Message, P-LSCPT, p. 2467.

[1074] Message, P-LSCPT, p. 2466, 2468 et 2472-2474.

[1075] HANSJAKOB, art. 269ter StPO, n° 2; HANSJAKOB, Jusletter-IT, n°1 et 10.

[1076] Message, P-LSCPT, p. 2398 et 2466-2468 et 2671.

[1077] CONSEIL FEDERAL, Rapport modification LSCPT, p. 41-42.

[1078] FF 2016 p. 1821; HANSJAKOB, art. 269ter StPO, n° 13-14; Message, P-LSCPT, p. 2473.

[1079] FF 2016 p. 1821; Message, P-LSCPT, p. 2467, 2471 et 2473.

1338 En outre, au vu de la gravité de l'atteinte à la vie privée, la mesure de surveillance consistant à agir activement sur le système informatisé ne peut être utilisée qu'en dernier recours lorsque les autres modes de surveillance sont restés sans succès, ou qu'ils n'auraient aucune chance d'aboutir ou rendraient la surveillance excessivement ardue[1080]. En somme, le législateur instaure une sorte de double subsidiarité, la première consistant à recourir aux autres moyens de contrainte prévus par le Code de procédure pénale avant d'employer les moyens de surveillances classiques, et la seconde de n'utiliser le logiciel d'espionnage qu'en dernier recours.

1339 Afin de limiter les risques d'atteinte considérable aux droits fondamentaux et/ou s'assurer que le Ministère public recourt à la surveillance au moyen de logiciels espions trop facilement, ce dernier doit tenir des statistiques sur l'utilisation de cette mesure de contrainte (art. 269*ter* al. 4 CPP), ce qui devrait permettre d'évaluer l'atteinte à la liberté personnelle, avec la précision que le coût d'utilisation devrait également limiter le recours à ces méthodes de surveillance[1081]. De même, l'art. 269*quater* CPP a été intégré au P-LSCPT qui prévoit notamment que seuls les programmes qui établissent des procès-verbaux peuvent être exploités afin d'éviter que les résultats soient alterés ou encore que le système de transmission soit sécurisé[1082].

1340 Nonobstant la nécessité d'édicter une base légale pour autoriser l'utilisation des chevaux de Troie dans le cadre de la surveillance secrète, quelques critiques ont été émises sur la base légale proposée au parlement dans l'avant-projet. En effet, une base légale qui autorise l'introduction d'un programme informatique doit respecter rigoureusement la précision. Or, la disposition proposée éludait quelques points qui ont été, en partie, rectifiés dans la P-LSCPT.

1341 Premièrement, malgré le fait que le ministère public doive indiquer quelles données il souhaite obtenir, la surveillance ne se limitait pas à un ou des programmes précis. Lors de la procédure de consultation, certains partis politiques ont émis l'idée de restreindre à certains secteurs, voire de déterminer si une "perquisition électronique" était acceptable ou si seules les données relatives au trafic pouvaient être relevées[1083].

1342 En effet, ni le rapport explicatif du Conseil fédéral, ni la base légale elle-même ne limitait la portée de l'utilisation du cheval de Troie. La seule contrainte qui existait concernait la nature des données qui devaient être utiles à la procédure.

[1080] FF 2016 p. 1821; HANSJAKOB, art. 269ter StPO, n° 8; Message, P-LSCPT, p. 2473.

[1081] HANSJAKOB, Jusletter-IT, n° 8 ; JAGGI, p. 280.

[1082] HANSJAKOB, Jusletter-IT, n° 7, 11 et 12.

[1083] Synthèse du résultat de la procédure de consultation LSCPT, p. 61-62.

1343 Ce constat engendrait la crainte de voir le logiciel d'espionnage utilisé comme une méthode de perquisition en ligne à l'insu de l'utilisateur, ce qui aurait constitué une atteinte extrêmement grave aux droits personnels et serait contraire à la pratique actuelle s'appuyant sur l'art. 245 CPP pour perquisitionner un ordinateur[1084].

1344 C'est pourquoi, l'art. 269*ter* CPP précise que la perquisition en ligne est interdite. L'introduction de GovWare ne pouvant être réalisé que pour lire des communications relevant de la téléphonie par Internet, intercepter les données communiquées, par exemple des messageries instantanées, et accéder aux e-mails[1085].

1345 Deuxièmement, aucune disposition ne prévoit les modalités d'effacement du cheval de Troie. Par conséquent, il n'est pas improbable qu'une fois la surveillance terminée, le logiciel reste actif sur l'ordinateur, ce qui, au regard du respect du droit à la vie privée, n'est pas tolérable. L'art. 269*ter* CPP n'introduit toujours pas de procédure d'effacement et le message du Conseil fédéral se limite à déclarer que l'autorité policière peut activer ou non le GovWare installé[1086].

1346 Troisièmement, la problématique la plus importante par rapport au principe de proportionnalité était le manque d'indication sur les infractions commises susceptibles d'enclencher la procédure de surveillance basée sur un logiciel espion.

1347 Le rapport explicatif de l'avant-projet précisait qu'au vu de la "double subsidiarité", toutes les infractions qui pourraient autoriser une surveillance classique de la correspondance "*sont susceptibles, dans un cas particulier, de présenter une gravité justifiant le recours au procédé de surveillance*". Néanmoins, aucune indication ne permettait de savoir en quoi consiste la gravité particulière qui est demandée[1087].

1348 De l'avis de certains parlementaires, il était préférable d'édicter une liste d'infractions corrélativement à ce qui prévaut pour la surveillance classique, ou tout du moins expliciter dans l'art. 269*ter* CPP que seules les infractions listées à l'art. 269 al. 2 let. a CPP étaient concernées. En effet, vue la gravité de l'atteinte à la sphère privée, l'interception et le décryptage des données devaient être autorisés dans des conditions très strictes. La liste des infractions énumérées à l'art. 269 al. 2 let. a à i CPP devaient par conséquent être limitée à des infractions très graves contre la vie ou l'intégrité corporelle, voire contre l'intégrité de

[1084] Infra Partie II, Chapitre 3, III, A, 3, c, iii, n° 2059 ss.

[1085] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 232; FF 2016 p. 1821; Message, P-LSCPT, p. 2467, 2471 et 2473.

[1086] FF 2016 p. 1821; Message, P-LSCPT, p. 2469.

[1087] Synthèse du résultat de la procédure de consultation LSCPT, p. 60.

l'Etat[1088]. Le législateur a été plus loin puisqu'il a réduit la liste des infractions à celles de l'art. 286 al. 2 CPP, plus restrictive, et donc plus conforme à la nature intrusive de ce mode de surveillance, largement supérieure à celle des méthodes classiques de surveillance[1089].

d) Les risques de l'utilisation des chevaux de Troie pour la valeur probante des données recueillies

1349 Aux fins de la preuve pénale, les remarques sur l'efficacité et les risques concernant la validité probatoire des autres modes de télécommunication valent de même pour les communications VoIP[1090]. S'ajoutent à ces remarques les risques provenant directement de la surveillance.

1350 L'intégration d'un programme pour intercepter et décrypter les données et accéder au système informatique n'est pas sans danger. Si l'autorité pénale utilise aisément l'introduction d'un logiciel espion, un tiers peut également y recourir pour contrôler, utiliser, voire modifier, le système d'un tiers surtout que l'art. 269*ter* CPP offre la possibilité d'introduire un programme complémentaire pour déjouer l'antivirus mettant à mal la sécurité de l'ordinateur ou du Smartphone[1091]. Ainsi, l'autorité crée une brèche importante tant dans la protection des données que dans la sécurité informatique. En niant ce fait et en expliquant que chaque programme est spécifique et n'est pas réalisé pour durer[1092], les spécialistes du domaine policier n'ont pas pris en considération tous les risques de fragilisation d'un système, les capacités des hackers et le fait que la structure du logiciel reste la même[1093].

1351 En outre, il n'est pas impossible que le logiciel espion utilisé par les autorités puisse faire son apparition sur la toile. Par exemple, si le logiciel est introduit dans l'ordinateur ou le Smartphone à l'aide d'un e-mail contenant une pièce jointe, il se peut que ledit e-mail soit transféré et contamine d'autres appareils. Dans cette hypothèse, tout un chacun pourra employer le cheval de Troie à titre particulier pour s'introduire et contrôler un appareil tiers.

1352 Les risques de voir des données personnelles à la portée de tiers n'est pas inexistant, ce qui peut laisser sceptique quant à l'emploi d'un tel système par l'autorité. Qui sera alors responsable des abus, du vol de données ou simplement de la brèche de sécurité

[1088] Synthèse du résultat de la procédure de consultation LSCPT, p. 62.

[1089] FF 2016 p. 1821; HANSJAKOB, art. 269ter StPO, n° 21-22; JAGGI, p. 279-280; Message, P-LSCPT, p. 2470 et 2472.

[1090] Supra Partie II, Chapitre 3, I, A, 4, a et b, n° 1254 ss et 1270 ss.

[1091] HANSJAKOB, art. 269ter StPO, n° 16; Message, P-LSCPT, p. 2468-2469.

[1092] JAGGI, p. 280; Message, P-LSCPT, p. 2468-2469.

[1093] HANSJAKOB, art. 269ter StPO, n° 8.

informatique créée? Le législateur nie également le problème des risques. Or, les spécialistes du monde scientifique ont uniquement déclaré que le programme finira tôt ou tard par se confronter à d'autre(s) logiciel(s) et que même si aucun dommage n'est constatable immédiatement, ce dernier terme démontre que, dans la durée, tel pourrait être le cas[1094].

1353 Tout logiciel implanté sur un système met en péril celui-ci. Ce constat est une évidence qui se prouve par le nombre de logiciels mettant à mal la sécurité informatique ou détruisant des données, voire créant des *bugs* de l'appareil. Quant aux logiciels espions, ils permettent autant de lire que d'intercepter, d'écrire ou de modifier des données. Dans ce contexte, il faut alors se poser la question de savoir comment l'autorité peut prouver l'authenticité des données recueillies. Par exemple, comment démontrer que la donnée n'a pas été téléchargée ou installée par le logiciel espion lui-même? A ce jour, aucune réponse n'a été apportée laissant un doute important quant à la viabilité de la preuve recueillie par cette méthode.

1354 Cela étant, nous le comprenons, ce mode de surveillance est essentiel au vu de l'utilisation toujours plus croissante de la téléphonie et/ou autre communication par Internet[1095]. Il est alors essentiel que le juge en charge du dossier constate qu'une brèche créée peut causer des modifications considérables des données. Il n'est alors par exclu que la conversation interceptée ne provienne pas de l'utilisateur surveillé ou que la donnée ait été modifiée, etc. Pour ce qui est des communications orales, le magistrat a néanmoins la possibilité de reconnaître la voix de la personne pour certifier que les dires sont authentiques. Nonobstant ce cas, les communications écrites ne peuvent aujourd'hui pas être certifiées, de même pour toutes les données contenues dans un ordinateur ou un Smartphone.

1355 En conséquence, la surveillance des communications VoIP se justifie au vu de l'informatisation de la société actuelle. Néanmoins, les risques qu'un tiers ait pris possession des données, ajoutés aux facteurs pouvant diminuer la preuve liée à la surveillance des autres types de communications[1096], les informations pouvant être obtenues ne fournissent en aucun cas une preuve absolue.

[1094] Message, P-LSCPT, p. 2469.

[1095] HANSJAKOB, art. 269ter StPO, n° 2, 3 et 24; HANSJAKOB, Jusletter-IT, n° 1; Message, P-LSCPT, p. 2470.

[1096] Supra Partie II, Chapitre 3, I, A, 4, a et b, n° 1254 ss et 1271 ss.

ii. La surveillance préventive

a) La réglementation prévue par le CPP

1356 En vertu des art. 269 ss CPP, la surveillance pénale de la correspondance a pour but de rechercher l'auteur d'une infraction ou de prouver l'existence d'une infraction préalablement commise. Ces dispositions n'ont pas pour but de servir à créer un soupçon excluant la possibilité d'effectuer une surveillance préventive[1097].

b) La réglementation prévue dans la LMSI

1357 La loi instituant des mesures visant au maintien de la sûreté intérieure (LMSI) est la norme principale réglant la surveillance préventive civile. Cette norme fédérale prévoit uniquement la surveillance aux fins de détecter un danger ou une menace pour la sécurité du pays.

1358 Les informations recherchées doivent permettre de prévenir et de lutter contre les dangers liés au terrorisme, au service de renseignements prohibé, à l'extrémisme violent ou à la violence lors de manifestations sportives (art. 2 al. 1 LMSI). En outre, ce type de surveillance ne peut être mis en œuvre sans des soupçons de commission d'une future infraction[1098].

1359 En revanche, la LMSI ne permet pas d'autoriser une surveillance aussi intrusive que celle connue dans le cadre de la procédure pénale[1099]. Cette limitation s'explique par le fait que, faute de commission d'une infraction, l'atteinte à la vie privée serait disproportionnée, et que la personne surveillée ne bénéficie pas des moyens de la procédure pénale pour remettre en cause la décision de surveillance.

1360 Par conséquent, en dehors du cadre de l'art. 2 LMSI, cette loi n'autorise pas la surveillance préventive dite de police.

[1097] EICKER, HUBER, p. 180; HANSJAKOB, BÜPF/VÜPF, art. 1 N 4; SCHMID, Praxiskommentar, art. 269 N 7.

[1098] Rapport explicatif LMSI II, p. 6.

[1099] Message, LMSI II, p. 4784.

c) Les réglementations cantonales sur la police

1361 La LMSI et le CPP ne prévoyant par la surveillance préventive, les observations policières pratiquées à titre préventif, telles que la prise de photos lors d'une manifestation, sont régies par les normes sur la police[1100].

1362 Depuis l'entrée en vigueur du Code de procédure pénale fédérale, la Confédération estime que les cantons qui réglementaient la surveillance préventive dans leur Code de procédure pénale doivent modifier leur législation sur la police[1101].

1363 Dans ce domaine de surveillance, le canton de Schwytz a fait office de modèle pour l'ensemble des cantons suisses dépourvus de législation, dès lors que le législateur schwytzois a déjà légiféré en la matière.

1364 A l'art. 9a al. 2 Polizeiverordnung[1102], la police peut recueillir des informations par le moyen des télécommunications lorsqu'il y a des raisons de penser qu'un acte criminel est commis ou pourrait être commis ou qu'un danger imminent pour la sécurité publique existe. En d'autres termes, la surveillance préventive des télécommunications n'est pas interdite de plein droit.

1365 Le canton de Zurich a également édicté des dispositions permettant les investigations secrètes préventives, notamment la surveillance des forums de discussion. Le Tribunal fédéral a confirmé la conformité avec les droits fondamentaux de l'art. 32e LPol/ZH dès lors que la compétence pour règlementer l'activité préventive de la police était du ressort des cantons et que l'art. 32e LPol/ZH conditionnait une telle surveillance à des délits graves renvoyant aux normes de procédures fédérales pour le surplus (art. 287-298 CPP)[1103]. En revanche, s'agissant de la surveillance sur Internet (art. 32f LPol/ZH), notre Haute Cour a retenu que la proportionnalité n'était pas respectée, puisque la surveillance des forums de discussion atteignait à la sphère privée d'un nombre important de personnes et donc d'individus qui ne sont pas soupçonnés et ne pourront l'être, ce d'autant que l'atteinte est estimée comme grave vu le nombre de données accessibles, qu'aucun régime d'autorisation n'était prévu et que les personnes touchées ne bénéficiaient d'aucune protection juridique postérieure[1104]. Cette disposition a donc été annulée. Au sujet de l'information en accord avec Thomas Hansjakob, il faut relever que l'arrêt du Tribunal fédéral est critiquable, puisque

[1100] JOSITSCH, MULLE, p. 497; RÉMY, p. 113; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 436-438; SCHUBARTH, Jusletter, n° 11.

[1101] SCHUBARTH, Jusletter, n° 11.

[1102] Verordnung über die Kantonspolizei (Polizeiverordnung) vom 22. März 2000, RS/SZ 520.110.

[1103] ATF 140 I 353, 366.

[1104] ATF 140 I 353, 374-378.

l'information de toutes les personnes surveillées nécessiterait de connaître l'identitée de celles-ci[1105]. Aussi, il serait préférable que l'information soit limitée aux personnes qui ont pu être identifiées et dont des charges sont retenues contre elles, sans quoi aucune enquête préventive ne serait autorisée et l'identification violerait à son tour les droits de la personnalité[1106].

1366 Jusqu'au 21 février 2013, Genève ne disposait pas de base légale dans la LPol pour ordonner, autoriser et justifier l'atteinte aux droits fondamentaux par la surveillance préventive. Depuis lors, avec entrée en vigueur le 20 avril 2013, la police genevoise peut effectuer des observations préventives (art. 21A LPol/GE).

1367 Il sied de relever que la loi genevoise prévoyait également une recherche préventive secrète (art. 21B aLPol/GE)[1107] et l'enquête sous couverture (art. 22 aLPol/GE)[1108]. Ces dispositions ont été invalidées par le Tribunal fédéral peu de temps après leur entrée en vigueur. Cela vaut de même pour l'alinéa 2 de l'art. 21A aLPol prévoyant la possibilité d'enregistrer les observations.

1368 En effet, dans un arrêt récent[1109], la Haute Cour a relevé que le CPP réglementait ces problématiques lorsque des soupçons laissaient présumer qu'une infraction avait été commise. Le Tribunal fédéral a également précisé qu'il n'existait aucune disposition pour surveiller une personne lorsqu'il n'existait pas encore de soupçons[1110].

1369 Cela étant, le Tribunal fédéral a estimé que la loi sur la police genevoise violait, en partie, les droits fondamentaux. En effet, les art. 21A al. 2, 21B et 22 aLPol/GE constituaient des

---

[1105] HANSJAKOB, forumpoenale 2015, p. 36.

[1106] HANSJAKOB, forumpoenale 2015, p. 36.

[1107] «*Afin de détecter la préparation de crimes ou de délits ou d'en empêcher la commission, la police peut engager un de ses membres, dont l'identité et la fonction ne sont pas décelables, au cours d'interventions brèves et sans utilisation d'une identité d'emprunt, aux conditions suivantes :a) il existe des indices sérieux qu'une infraction pourrait être commise;b) d'autres mesures de recherche d'information n'ont pas abouti, n'auraient aucune chance d'aboutir ou seraient excessivement difficiles.*»

[1108] «*1 Avant l'ouverture d'une procédure pénale et afin de détecter la préparation de crimes ou de délits ou d'en empêcher la commission, la police peut mener des enquêtes sous couverture aux conditions suivantes :a) il existe des indices sérieux qu'une infraction pourrait être commise; b) la gravité de l'infraction considérée le justifie; c) d'autres mesures de recherche d'information n'ont pas abouti, n'auraient aucune chance d'aboutir ou seraient excessivement difficiles. 2 Seul un membre de la police peut procéder à des actes d'enquête sous couverture.3 Le commandant peut doter l'agent infiltré d'une identité d'emprunt.4 La mise en œuvre d'actes d'enquête sous couverture est soumise à l'autorisation du Tribunal administratif de première instance. 5 L'article 151 du code de procédure pénale s'applique par analogie.*»

[1109] ATF 140 I 381.

[1110] ATF 140 I 381, 389 et 392.

atteintes à la sphère privée, soit notamment aux relations sociales et à la communication avec autrui ainsi qu'à l'autodétermination, si bien que ces dispositions devaient respecter l'art. 36 Cst.

1370 Or, le Tribunal fédéral a constaté que l'atteinte à la sphère privée prévu par les dispositions précitées ne respectait pas le principe de la proportionnalité. En effet, l'art. 21A al. 2 aLPol/GE prévoyait la possibilité d'enregistrer les observations sans qu'une communication *a posteriori* soit obligatoire. L'art. 21B LPol/GE a été considéré comme violant la proportionnalité dès lors qu'aucune autorisation préalable d'une autorité n'était requise pour effectuer des recherches préventives secrètes et la communication *a posteriori* n'était pas non plus prévue par la disposition légale[1111]. Ce constat vaut de même pour l'art. 22 aLPol/GE prévoyant l'enquête sous couverture.

1371 La Haute Cour a néanmoins admis que moyennant le respect des conditions de l'art. 36 Cst les bases légales genevoises concernant la surveillance préventive était adéquate, voire même utile[1112]. La nouvelle loi sur la Police (nLPol/GE) prévoyait également des dispositions analogues aux articles 21A, 21B et 22 LPol/GE qui ne respectaient pas la volonté du Tribunal fédéral[1113]. C'est pourquoi, un projet de modification de la LPol/GE a été présenté au Conseil d'Etat en date du 7 mai 2015 afin d'introduire des articles conforment aux conditions jurisprudentielles permettant l'observation préventive, les recherches secrètes préventives et/ou les investigations secrètes préventives (art. 56 al. 1, 57 al. 1 et 58 al. 1 P-LPol/GE)[1114].

1372 En revanche, aucune disposition n'a été édictée à Genève en ce qui concerne la surveillance préventive des télécommunications. Ainsi, pour les cantons dépourvus de législation ayant trait à la prévention des risques par la surveillance des télécommunications qui souhaite légiférer, il est à notre avis indispensable, conformément aux jugements du Tribunal fédéral[1115], que la norme cantonale instaure un régime d'autorisation pour protéger au mieux la vie privée des individus ainsi qu'une communication *a posteriori*. D'ailleurs, la législation schwytzoise renvoie à la LSCPT qui elle-même renvoie aux art. 274-279 CPP pour ce qui est de la procédure de mise sous surveillance[1116]. La surveillance préventive à Schwytz est donc

[1111] ATF 140 I 381, 394.

[1112] ATF 140 I 381, 384-385.

[1113] Projet de loi modifiant la loi sur la police (LPol) - PL 11664, p. 3.

[1114] Projet de loi modifiant la loi sur la police (LPol) - PL 11664, p. 1 et 2.

[1115] ATF 140 I 353, ATF 140 I 381.

[1116] Verordnung über die Kantonspolizei (Polizeiverordnung) vom 22. März 2000, RS/SZ 520.110.

soumise à autorisation. Conséquemment, sans autorisation, les données issues d'une telle surveillance sont inexploitables (art. 277 CPP *cum* 141 al. 1 CPP).

1373 A défaut de bases similaires à celles schwytzoises et/ou, dans un avenir proche, genevoises[1117], la police cantonale ne peut pas procéder à ce type de surveillance, conséquemment ne peut pas exploiter une information qu'elle aurait obtenue illicitement par ce mode d'investigation. Bon nombre de cantons sont aujourd'hui dans cette situation de flou juridique en ce qui concerne la surveillance préventive.

1374 Ainsi, alors même que des présomptions existent, les autorités policières de certains cantons n'ont aucun moyen de surveiller à titre préventif et d'avoir des soupçons pouvant enclencher la procédure pénale. Il est donc à prévoir qu'un certain nombre de commissions d'actes délictuels ne pourront être empêchés et que certaines infractions resteront impunies, hormis si des preuves sont relevées et exploitables subséquemment, jusqu'à l'édiction d'une norme cantonale suffisante.

d) La loi sur le renseignement (LRens), non-entrée en vigueur

1375 Le Service de renseignement civil de la Confédération (SRC) procède à la recherche d'informations, les analyse, les évalue et les transmets aux décideurs à tous les échelons afin de leur fournir les informations dont ils ont besoin pour pouvoir accomplir leurs tâches de conduite en temps utile et en fonction de la situation[1118]. Ce service fait partie intégrante de la politique sécuritaire de la Suisse.

1376 Actuellement, la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI) ainsi que la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC)[1119], qui est le pendant de la LMSI en ce qui concerne les préventions des menaces extérieures contre la sûreté en Suisse, réglementent les tâches du SRC.

1377 Depuis octobre 2010, des travaux ont été entrepris pour élaborer une nouvelle loi sur le renseignement qui n'entrera pas en vigueur avant l'année 2017, étant précisé que le projet a et le message du Conseil fédéral ont été approuvé le 19 février 2014. Cette loi doit remplacer

[1117] Verordnung über die Kantonspolizei (Polizeiverordnung) vom 22. März 2000, RS/SZ 520.110; Projet de loi modifiant la loi sur la police (LPol) - PL 11664.

[1118] SERVICE DE RENSEIGNEMENT DE LA CONFEDERATION SRC, *Brochure – le Service de renseignement de la Confédération SRC*, Berne 2013, p. 5.

[1119] Loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC), RS 121.

la LMSI et la LFRC en créant une base légale formelle uniforme qui ne différencie plus les menaces émanant de l'intérieur et de l'étranger.

1378 Le texte de la loi sur le renseignement a été publié dans la Feuille fédérale le 6 octobre 2015 fixant un délai référendaire au 14 janvier 2016. Le référendum ayant abouti, le peuple devra voter sur l'entrée en vigueur de cette loi, au plus tôt le 5 juin 2016[1120].

1379 La loi sur le renseignement vise également à offrir un cadre légal suffisant aux activités spéciales de renseignement, telles que la surveillance des télécommunications, l'observation des personnes dans des lieux privés et l'accès à des systèmes et/ou des réseaux informatiques (art. 23 ss LRens). En effet, dans le domaine du terrorisme, de l'espionnage ou pour tout intérêt essentiel de la Suisse, ni la LMSI ni la LFRC ne permet au SRC d'assurer ses tâches de prévention face aux protagonistes qui menacent la sûreté intérieure et extérieure de la Suisse. Par exemple, actuellement, la LMSI n'autorise pas, à titre préventif, le SRC à surveiller la correspondance par poste et télécommunication, d'observer des lieux qui ne sont pas librement accessibles au public, notamment au moyen d'appareils techniques de surveillance ou de s'introduire dans des systèmes informatiques. Cette impossibilité crée d'importante lacune dans le dispositif de prévention, extensivement de sécurité de la Suisse.

1380 La LRens doit permettre de combler ces lacunes en créant une base légale au sens formelle suffisante pour restreindre les droits fondamentaux pouvant être touchés par certaines mesures de surveillance préventives.

1381 Ainsi, la loi sur le renseignement doit permettre au SRC d'agir préventivement et de rechercher toutes les informations utiles (art. 1 al. 1 et 2 LRens), afin de prévenir les menaces et les dangers, tout en respectant les libertés constitutionnelles ou, tout du moins, leurs conditions de restriction[1121].

1382 Relevons toutefois que dans le projet d'origine LMSI II, le Parlement avait refusé d'introduire les dispositions sur la surveillance préventive du trafic par poste et télécommunication, l'engagement d'appareil de surveillance dans la sphère privée, etc[1122]. Ces dispositions ont été remaniées et complétées dans la LRens, ce dont le législateur a approuvé afin de permettre l'introduction des mesures de surveillances soumises à autorisation au sens des art. 23 et ss LRens.

[1120] Informations disponibles sur le site du DDPS : http://www.vbs.admin.ch/ [consulté le 08.05.2016].

[1121] Rapport sur l'avant-projet LRens, p. 7

[1122] Rapport sur l'avant-projet LRens, p. 2

1383 Relevons encore que les opposants, notamment "L'alliance contre l'Etat fouineur", ont récolté environ 60'000 paraphes. Cette engoument s'explique probablement suite à l'affaire de la NSA et aux révélations d'Edward Snowden et la volonté de la population de sauvegarder au maximum sont droit à la sphère privée[1123].

iii. L'IMSI- Catcher

a) La technique de l'IMSI-Catcher en quelques mots

1. La description de l'IMSI-Catcher

1384 L'IMSI-Catcher est un nouveau dispositif de surveillance des téléphones mobiles.

1385 Techniquement, l'IMSI-Catcher est un boîtier qui simule une antenne GSM et se place virtuellement entre l'antenne relais et celle du téléphone mobile[1124]. Ainsi, tout téléphone mobile se trouvant dans la zone de couverture de l'IMSI-Catcher est automatiquement mis en contact avec le dispositif. Le numéro IMSI et IMEI est alors à la portée de l'appareil, ce qui permet de connaître l'utilisateur du téléphone, de le localiser et, depuis la seconde version de l'appareil, d'écouter les conversations[1125].

1386 Relevons encore que cette technique ne nécessite pas l'intervention de l'opérateur[1126]. Ainsi, cette méthode de surveillance offre une plus grande liberté et une facilité pour le service d'enquête.

2. Les limites techniques

1387 Actuellement, l'IMSI-Catcher a quelques limites techniques que nous n'exposerons pas exhaustivement[1127].

1388 En premier lieu, l'IMSI-Catcher fonctionnant à l'aide d'une simulation d'antenne, le téléphone mobile n'est plus en contact avec l'opérateur. Aussi, aucune communication entrante ne peut parvenir à l'utilisateur qui fait l'objet de la surveillance.

[1123] L'Hebdo, *Le peuple décidera de l'avenir de la loi sur le renseignement*, article du 31 décembre 2015.

[1124] FOX, p. 213; Message, P-LSCPT, p. 2464; MÉTILLE, Jusletter, n° 25.

[1125] DE SAUSSURE, n° 6-10; FOX, p. 213.

[1126] DE SAUSSURE, n° 4; Message, P-LSCPT, p. 2464; MÉTILLE, Thèse, p. 40; STROBEL, p. 13-17.

[1127] A ce sujet, voir: STROBEL, p. 14-16.

1389 En second lieu, le dispositif de surveillance ne peut être activé que si le téléphone est au moins en veille. Il faut par conséquent que le téléphone soit nécessairement actif, ce qui restreint un certain nombre de cas où l'IMSI-Catcher est réellement utile.

1390 En troisième lieu, certains téléphones mobiles affichent un symbole lorsque l'IMSI-Catcher est activé et qu'il capte le téléphone. Toute personne un tant soit peu attentive peut donc voir le symbole sur son appareil mobile et savoir qu'elle est surveillée.

1391 En quatrième lieu, plus il y a de téléphones mobiles dans le périmètre de fonctionnement de l'IMSI-Catcher, plus le nombre d'interceptions de numéros IMSI ou IMEI est important[1128]. Il faut alors faire des recoupements pour trouver la personne cible de la surveillance. Par conséquent, la surveillance à l'aide de cette technique peut apporter son lot de difficultés et d'incertitudes.

1392 Enfin, l'IMSI-Catcher ne peut fonctionner que sur le réseau GSM puisqu'il exploite une faille de ce protocole. Néanmoins, actuellement, deux protocoles sont souvent employés pour la téléphonie mobile: le protocole GSM et l'UMTS[1129]. Dès lors, si le protocole UMTS se développe aux dépens du protocole GSM, l'utilisation d'IMSI-Catcher sera totalement obsolète[1130].

b) L'utilisation de l'IMSI-Catcher au regard du droit suisse

1393 Juridiquement, il ne fait aucun doute que l'IMSI-Catcher est un moyen de surveillance des télécommunications. La question que soulève l'utilisation de ce dispositif est de savoir s'il s'agit d'une méthode classique de surveillance de la correspondance (art. 269 ss CPP) ou s'il s'agit d'une autre mesure de technique de surveillance (art. 280 let. a CPP) au regard du droit procédural actuel.

1394 L'IMSI-Catcher est un appareil qui permet notamment d'écouter des conversations à distance. En revanche, il n'emprunte pas les installations téléphoniques pour pouvoir fonctionner. D'après Bernhard Sträuli: "[…] *lorsque l'utilisation d'un appareil technique vient se greffer sur une installation terminale de télécommunication* […] *parce que ces procédés ne requièrent par l'intervention d'un opérateur de télécommunication* […]*, ils relèvent exclusivement*

[1128] Message, P-LSCPT, p. 2465.

[1129] BOVET, p. 694.

[1130] DE SAUSSURE, n° 12; FOX, p. 215. *A contrario*: MEYER, WETZEL, p. 92-97; STROBEL, p. 19.

de l'utilisation d'appareils techniques de surveillance."[1131]. Par conséquent, il ne nous semble pas approprié de reconnaître cette technique comme un moyen de surveillance classique (art. 269 ss CPP).

1395 Au sens de l'art. 280 CPP, les appareils techniques de surveillance se définissent à la lumière des art. 179*bis*, 179*quater* et 179*octies* CP. Cette notion comprend tous les procédés acoustiques ou optiques tels que micros, magnétophones, appareils d'écoutes à distance, etc.[1132] Cette définition intègre vraisemblablement l'IMSI-Catcher, mais pas toutes les fonctionnalités de cette technique de surveillance. Ainsi, l'objet de l'art. 280 CPP n'intègre pas tous les buts de l'IMSI-Catcher.

1396 Quant aux écoutes des communications sortantes, la surveillance effectuée par l'IMSI-Catcher correspond à la surveillance en temps réel (art. 16 let. a OSCPT) à la différence près que ni le fournisseur du service de télécommunication, ni le SCPT n'ont en réalité besoin d'agir, ce qui pourrait accroître la confidentialité des données interceptées. L'interception des conversations sortantes entre dans le champ d'application de l'art. 280 let. a CPP, mais uniquement à l'encontre d'un prévenu (art. 281 al. 1 CPP). En revanche, il est impossible d'utiliser ce dispositif à des fins probatoires contre un prévenu en détention (art. 281 al. 3 let. a CPP) ou pour surveiller les locaux ou les véhicules d'un tiers appartenant à l'une des catégories visées aux art. 170 à 173 CPP (art. 281 al. 3 let. b CPP).

1397 S'agissant de l'identification du titulaire du raccordement, la capture du numéro IMSI et IMEI peut faire l'objet d'une surveillance (art. 15 al. 1 LSCPT et art. 19 OSCPT) moyennant le concours du fournisseur de services de télécommunication. Premièrement, parce que l'IMSI-Catcher ne nécessite par le concours du fournisseur, et deuxièmement, parce que l'art. 280 CPP ne prévoit pas l'utilisation d'une autre technique de surveillance pour identifier le titulaire d'un raccordement, l'IMSI-Catcher ne peut donc pas actuellement être employé à cette fin faute de base légale suffisante.

1398 En ce qui concerne la localisation à l'aide de l'IMSI-Catcher, l'art. 280 let. c CPP la permet. Ce constat crée une incohérence. En effet, les numéros IMSI et IMEI peuvent être employés pour localiser un prévenu, mais non pas pour l'identifier. Pour une meilleure sécurité juridique, et parce que l'identification d'un utilisateur n'est pas plus invasive que sa localisation ou

[1131] STRÄULI, p. 117.

[1132] ATF 133 IV 249, 253-254 = JdT 2009 IV 10, 14-15; HURTADO POZO, art. 179*bis* N 2206; STRATENWERTH, JENNY, BOMMER, p. 268-269.

l'écoute de ses conversations, il nous semble approprié d'autoriser par le biais de l'art. 280 CPP l'identification de l'utilisateur[1133].

1399 Se pose encore la question du clonage de l'antenne relais par l'IMSI-Catcher qui impose qu'aucune communication entrante ne puisse parvenir à son destinataire.

1400 En principe, il est illicite de perturber le trafic des communications[1134]. Cependant, l'art. 34 al. 1*ter* LTC prévoit la possibilité d'utiliser des brouilleurs. D'après Stéphane Bondallaz, cet article ne doit s'appliquer que subsidiairement et pour un laps de temps restreint[1135].

1401 La Cour constitutionnelle allemande s'est prononcée en faveur de l'utilisation d'un IMSI-Catcher, notamment en déclarant que l'interruption du réseau subie par l'utilisateur est insignifiante et correspond à une coupure réseau normale qui peut survenir sur un réseau de téléphonie mobile[1136]. L'utilisation de l'IMSI-Catcher ne paraît donc pas illicite de ce point de vue[1137].

1402 *A priori*, l'utilisation de l'IMSI-Catcher n'est donc pas illégale et, à certaines conditions, peut être autorisée en se fondant sur l'art. 280 let. a et c CPP.

1403 Néanmoins, le législateur a, à juste titre, relevé qu'il était indispensable pour les autorités de poursuite pénale de pouvoir identifier un utilisateur au moyen de l'IMSI-Catcher et qu'une telle mesure de contrainte atteignait moins gravement aux droits fondamentaux que la localisation[1138]. C'est pourquoi, dans le cadre de la révision de la LSCPT, une base légale expresse a été prévue à l'art. 269*bis* CPP pour autoriser la police sur ordre du ministère public à utiliser des appareils particuliers, tels que l'IMSI-Catcher[1139]. Si cet article entre en vigueur, et contrairement à ce qui prévaut aujourd'hui, il sera alors possible d'identifier, grâce aux numéros IMSI et IMEI, l'utilisateur de téléphonie, étant relever que l'art 269*bis* CPP prévoit également spécifiquement le recours à l'IMSI-Catcher pour écouter et/ou enregistrer les conservations ou encore localiser les utilisateurs sans requérir l'intervention de l'opérateur[1140].

[1133] Dans ce sens: DE SAUSSURE, n° 51.

[1134] BONDALLAZ, protection des personnes, p. 345; MÜLLER, SCHEFER, p. 171 ss.

[1135] BONDALLAZ, protection des personnes, p. 346.

[1136] BVerfG, 2 BvR 1345/03 vom 22.8.2006, §83.

[1137] DE SAUSSURE, n° 58.

[1138] Message, P-LSCPT, p. 2464.

[1139] CONSEIL FEDERAL, Rapport modification LSCPT, p. 43; Message, P-LSCPT, p. 2464.

[1140] FF 2016 1821, p. 1841; Message, P-LSCPT, p. 2464.

1404 Le classement de cette disposition légale au sein de la surveillance par poste et télécommunication a été justifié par le fait que cette méthode de surveillance permet d'obtenir des données relevant de la correspondance par télécommunication, même si le fournisseur et/ou le service n'a aucun rôle à jouer[1141].

1405 Il sied encore de relever qu'au vu de l'atteinte aux droits fondamentaux créée par cette méthode de surveillance et de l'importance d'éviter au maximum que des personnes innocentes soient entravées par cette mesure dès lors qu'elles se trouvent simplement dans le champ d'action de l'IMSI-catcher, l'art. 269*bis* CPP prévoit que le Ministère public doit disposer d'une autorisation du Tribunal des mesures de contrainte (art. 274 CPP) et que les conditions suivantes doivent être respectées, à savoir : que les conditions requises en vertu de l'art. 269 CPP pour une surveillance classique soient remplies (let. a); que l'utilisation de l'IMSI-Catcher soit subsidiaire à toutes les autres méthodes classiques dès lors que ce moyen ne doit pas remplacer les modes de surveillance actuels, mais les compléter en tant que besoin[1142] (let. b); et que le Ministère public ait obtenu l'autorisation octroyée pour un utilisateur défini ainsi que pour une utilisation d'un certain nombre d'appareils et délivrée par l'Office fédéral des télécommunications (OFCOM) (let. c *cum* art. 32*a* et 34 al. 1ter LTC, art. 6 al. 4 OIT et 49 ss de l'ordonnance du 9 mars 2007 sur la gestion des fréquences et les concessions de radiocommunication (OGC)), avec la précision que la demande doit contenir les paramètres techniques afin que l'OFCOM puisse évaluer les risques de perturbation[1143].

1406 Par conséquent, si la surveillance est autorisée et que les données sont utiles à la procédure pénale (art. 276 et 277 *a contrario* CPP), moyennant les avantages et les inconvénients des techniques de surveillance[1144], notamment quant à l'atteinte à la sphère privée et à la restriction actuelle du champ d'application de l'art. 280 CPP, l'utilisation de l'IMSI-Catcher est possible et offre une technique supplémentaire pour obtenir des informations relatives aux communications. De surcroît, si l'art. 269*bis* CPP entre en vigueur, rien n'est moins sur au vu du délai référendaire, du fait que des opposants montent d'ores et déjà au front contre la modification de la LSCPT[1145] et du nombre de signatures atteint contre la LRens[1146], alors le Ministère public pourra requérir une surveillance des communications au moyen de ce dispositif pour écouter et/ou enregistrer les communications, identifier l'utilisateur ou encore localiser l'appareil concerné.

[1141] Message, P-LSCPT, p. 2464.

[1142] FF 2016 1821, p. 1841; Message, P-LSCPT, p. 2464-2465.

[1143] Message, P-LSCPT, p. 2465.

[1144] Supra Partie II, Chapitre 3, I, A, 4, a et b, n° 1254 ss et 1271 ss.

[1145] Informations disponibles sur le site internet : https://www.lscpt.ch [consulté le 28.04.2016].

[1146] Supra Partie II, Chapitre 3, I, A, 4, c, ii, d), n° 1378.

B. La vidéosurveillance

1407 Aujourd'hui, la vidéosurveillance est présente un peu partout: établissements privés ou publics, parkings, transports publics, voies publiques, etc. Ce moyen technique permettant de voir à travers l'œil d'une caméra s'est largement développé sur le domaine public, privé et dans le monde policier et judiciaire.

1408 Hantée par le spectre du "Big Brother" et l'aspect sécuritaire hors-norme, l'ampleur prise par cette technique s'est accompagnée de l'inquiétude tant quant au respect des droits fondamentaux qu'à la prise en compte de la qualité dissuasive et/ou probatoire des images filmées.

1409 Outre l'usage dissuasif ou répressif des systèmes de caméra, ce moyen visuel peut servir aux fins d'enregistrer des auditions de témoins (art. 154 al. 4 let d CPP) ou plus généralement, certains actes de procédure (art. 76 al. 4 CPP). L'utilisation du dispositif audiovisuel durant la procédure permet de collecter des preuves exploitables qui sont jugées idéologiquement comme infaillibles.

1410 La présente partie définit le cadre technique et légal de la vidéosurveillance et, en *excursus*, de l'enregistrement audiovisuel, cherche à déterminer la valeur probatoire des enregistrements administrés comme preuve et tente d'exposer les avantages ou inconvénients de cette technique.

1. L'introduction

a. La définition de la vidéosurveillance

1411 La vidéosurveillance désigne l'observation de lieux, de comportements ou de personnes à l'aide d'un dispositif optique électronique[1147]. Il s'agit d'un système technique composé d'une caméra et d'un moniteur distant géographiquement – même de quelques mètres – qui sont reliés par un moyen technique de transmission et dont les images transférées peuvent ou non faire l'objet d'un enregistrement[1148].

[1147] BAUSCH, p. 3

[1148] BAUER, FREYNET, p. 11; BÜLLESFELD, p. 6; FICHET-BOYLE, p. 205.

1412 Ainsi, l'utilisation de la surveillance vidéo fait appel à diverses technologies: la capture, la transmission et, éventuellement, l'archivage et l'analyse des données[1149].

1413 En d'autres termes, la vidéosurveillance est une technique de surveillance permettant d'obtenir des images, de les visualiser et/ou de les archiver afin de pouvoir les utiliser en cas de besoin, notamment pour élucider une infraction ou identifier l'auteur d'un acte délictuel, voire pour servir de preuve.

b. Les divers types de vidéosurveillance

1414 La vidéosurveillance peut être installée par une personne physique ou morale ou encore par une autorité. Elle englobe toute une série de systèmes qui s'utilisent à diverses fins. En outre, elle s'accompagne ou non d'un enregistrement des images. En fonction de ces trois critères, la protection des droits fondamentaux et le régime juridique de mise en œuvre varient substantiellement. C'est pourquoi il faut distinguer les divers types de vidéosurveillance pouvant exister en Suisse.

i. La vidéosurveillance exercée par les personnes privées et par les autorités publiques

1415 En réponse aux menaces d'insécurité, les autorités fédérales ou cantonales et les particuliers ont massivement déployé des systèmes de surveillance caméra sur le domaine privé ou public[1150]. Cependant, selon la qualification juridique de l'auteur de la vidéosurveillance, les domaines pouvant être surveillés diffèrent.

1416 Un particulier est habilité à surveiller sa propriété alors que les autorités cantonales ou fédérales peuvent surveiller le domaine public. En revanche, un particulier n'est en général pas autorisé à filmer le domaine public; corrélativement, une autorité publique, exception faite de la police en cas d'infraction pénale, n'est pas habilitée à employer la vidéosurveillance dans un lieu privé sans l'assentiment de l'ayant-droit[1151]. Il faut par conséquent définir ces divers lieux pour connaître où une personne privée ou morale et où une autorité officielle peuvent agir.

[1149] RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 31-36. Infra Partie II, Chapitre 3, I, B, 1, c, n° 1439 ss.

[1150] KLAUSER, CCTV, p. 148-149.

[1151] Infra Partie II, Chapitre 3, I, B, 2, c, i, n° 1496 ss; Infra Partie II, Chapitre 3, I, B, 2, c, ii, a) et c), n° 1530 et 1546-1547.

1417 Le domaine privé comprend la partie du territoire appartenant à une personne physique ou morale dont elle peut disposer librement, soit sa propriété (art. 641 CC).

1418 Si le domaine privé appartient aux personnes physiques ou morales, l'espace public échoit aux collectivités publiques et à ses organes. Pour la doctrine et la jurisprudence, "*le domaine public comprend l'ensemble des choses et des biens qui ne sont pas affectés à une finalité particulière par l'Etat et qui peuvent être utilisés par les particuliers sans interventions des agents publics, en principe de manière libre, égale et gratuite*", ce qui comprend les rues, les places, les parcs, etc. A ceci s'ajoute le patrimoine administratif de l'Etat – biens mobiliers ou immobiliers – lui permettant de remplir ses tâches, tels que les hôpitaux, musées, écoles, parkings, etc.[1152].

1419 Cette démarcation entre domaine privé et public implique quelques inégalités. Par exemple, alors que les commerçants d'une rue piétonne devront faire la demande aux autorités s'ils désirent installer un système de caméra de surveillance pour se prémunir contre les incivilités extérieures; la situation est différente pour les commerçants regroupés dans un centre commercial, dès lors qu'ils sont seuls à décider.

1420 En accord avec une partie de la doctrine, la frontière entre le domaine privé et public doit être parfois atténuée à l'aide de la notion d'"*espace à usage public*" qui intègre les lieux ouverts au public issus du secteur privé ou public. Il ne s'agit alors plus de distinguer les lieux en fonction du statut juridique de l'exploitant de la vidéosurveillance, mais de son usage[1153]. En revanche, seule la propriété foncière est opérante pour déterminer l'applicabilité des droits relatifs à la mise en place d'un système de surveillance caméra.

ii. La finalité de la vidéosurveillance

1421 L'objectif visé par la mise en œuvre d'un système de vidéosurveillance amène la doctrine à différencier trois, voire quatre, types de surveillance des lieux publics ou privés: invasive, dissuasive, répressive et d'observation[1154].

[1152] AUER, FLÜCKIGER, p. 926; HOTTELIER, SJ 2002, p. 124 et 126; MOOR, POLTIER, p. 253 ss; RUEGG, p. 3; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 47.

[1153] GHORRA-GOBIN, p. 50; LÉVY J., p. 337; RUEGG, p. 4.

[1154] BAERISWYL, Videoüberwachung, p. 27; BÜLLESFELD, p. 19-20 et 31-35; CUSSON, Nouvelles technologies, p. 69; DFJP, Rapport vidéosurveillance, p. 9; FLÜCKIGER, p. 197; REMY, p. 110; RUEGG, p. 6; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 7.

1422 La vidéosurveillance invasive a pour but de surveiller un individu déterminé ayant commis une infraction ou soupçonné d'en commettre une prochainement. Pour être efficace, cette surveillance est secrète. Les normes de droit pénal (art. 179*quater* et 179*octies* CP), de procédure pénale (art. 280 ss CPP) et de droit policier – surveillance préventive – réglementent la mise en œuvre d'une telle mesure.

1423 La vidéosurveillance dissuasive doit être visible pour atteindre son but[1155], c'est-à-dire d'éviter les comportements illicites en dissuadant les auteurs d'agir contrairement à la loi et à la morale. Nonobstant son usage par les particuliers, ce type de surveillance fait partie intégrante des tâches policières et est donc réglementé par le droit en la matière.

1424 Les mesures de surveillance répressive peuvent être issues de la vidéosurveillance dissuasive ou invasive. Dès qu'un système d'enregistrement est intégré au dispositif de vidéosurveillance, indépendamment du but premier invasif ou dissuasif, les images collectées peuvent être utilisées *a posteriori* comme preuve pour établir les faits ou confondre le coupable[1156]. Cette mesure de surveillance intervient dans le cadre d'une procédure pénale et doit donc respecter les dispositions générales sur la preuve (art. 139 ss CPP) et les moyens de contrainte (art. 196 ss CPP), ainsi que les dispositions spécifiques sur les autres mesures techniques de surveillances (art. 280 ss CPP).

1425 La vidéosurveillance d'observation est notamment employée pour surveiller le trafic routier. Elle ne vise pas à modifier le comportement des usagers et les enregistrements ne contiennent généralement pas de données personnelles. Il s'agit par exemple uniquement de surveiller le flux des véhicules ou de permettre l'envoi rapide d'une patrouille en cas d'accident. Néanmoins, la résolution toujours plus performante offre la possibilité d'identifier les individus, notamment par leur numéro d'immatriculation[1157]. Il paraît donc vraisemblable que la vidéosurveillance d'observation devienne prochainement une sous-catégorie de la vidéosurveillance invasive ou dissuasive.

iii. L'agencement du système de vidéosurveillance

1426 Certains auteurs de doctrine distinguent, à juste titre, trois groupes de vidéosurveillance dépendamment de leur agencement[1158].

[1155] BAERISWYL, Videoüberwachung, p. 27; BÜLLESFELD, p. 22 et 34; MÉTILLE, Thèse, p. 84.

[1156] BÜLLESFELD, p. 23 et 32; MÜLLER, SCHEFER, p. 173.

[1157] MÜLLER, WYSSMANN, p. 542; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 41.

[1158] BAUSCH, p. 3-4; BÜLLESFELD, p. 20-22; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 89.

1427 La vidéosurveillance non informatisée est une surveillance directe des personnes permettant de les identifier sans enregistrement de données[1159]. Il s'agit d'une pure transmission d'image sur un moniteur qui demande une présence constante d'un personnel de surveillance.

1428 En grande majorité, ce type de vidéosurveillance est utilisé comme méthode de dissuasion.

1429 En outre, si la caméra est munie d'un zoom optimal, il est toujours possible d'identifier un individu.

1430 Ce type de vidéosurveillance sans enregistrement ne constitue pas en soi une ingérence à la sphère privée des individus[1160].

1431 La vidéosurveillance avec enregistrement simple occasionne, comme son nom l'indique, l'enregistrement des données – images filmées – qui sont automatiquement effacées après une brève période. Ainsi, il est possible d'admettre ultérieurement les informations enregistrées comme moyen de preuve.

1432 Ce moyen de vidéosurveillance avec l'effacement automatique atteint aux libertés fondamentales de manière plus ou moins légère selon la durée de conservation[1161].

1433 La vidéosurveillance avec traitement informatisé permet de coupler les données enregistrées avec une ou des bases de données – biométrique, policière, etc. – afin d'établir un profil de la personnalité[1162]. A l'aide du traitement informatique des images, il est également possible d'améliorer les contrastes, d'élargir une section de l'image, etc. Ce potentiel permet une meilleure évaluation des données recueillies et par conséquent une mise en perspective plus probante avec d'autres informations préalablement enregistrées.

1434 Ce type de vidéosurveillance atteint sans conteste aux droits et libertés fondamentaux[1163].

[1159] BÜLLESFELD, p. 20; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 89.

[1160] CourEDH, Affaire *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, 44647/98, § 59; CourEDH, Affaire *Calmanovici c. Roumanie*, arrêt du 1er juillet 2008, 42250/02, § 130.

[1161] ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65-67; CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 59-60.

[1162] AUER, FLÜCKIGER, p. 925; BÜLLESFELD, p. 21-22; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 89.

[1163] ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65-67; CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 59-60.

iv. Excursus: l'enregistrement audiovisuel

1435 Le Code de procédure pénale (art. 76 al. 4 et 154 al. 4 CPP) prévoit la possibilité d'enregistrer sur un support visuel, audio ou audiovisuel certains actes d'instruction, notamment les témoignages ou les déclarations effectuées par la partie plaignante. Dans ce cadre, la capture des images sert non seulement à compléter le procès-verbal (art. 77 let. e et g CPP) [1164], mais peut également être administrée au procès.

1436 L'utilisation d'une caméra doit permettre notamment: d'éviter la confrontation entre l'accusation et la défense, de fournir un moyen de preuve en évitant ainsi les ouïes-dires et de fournir à la Cour les passages exacts des déclarations faites lors de la procédure d'enquête ou d'investigation, voire de limiter le nombre d'auditions de la victime ou d'interrogatoires des témoins[1165].

1437 Grâce à la technologie audiovisuelle, les gestes, les mimiques physiques et le comportement général de l'individu entendu sont enregistrés. Ces indices peuvent permettre de déterminer si la vérité est réellement apportée ou si une gêne existe. Ainsi, le tribunal peut apprécier le degré de spontanéité des déclarations de la personne concernée et fonder sa décision sur ce qu'il peut voir à travers les images[1166].

1438 Outre le visuel directe des formulations et gestuelles de l'individu, l'enregistrement audiovisuel accroît la précision de la traduction et assure que la procédure encadrant l'interrogatoire ait bien été respectée[1167].

1439 Ainsi, l'enregistrement audiovisuel est un outil précieux pour obtenir la perception la plus exacte des interrogatoires, notamment lorsqu'aucune confrontation directe n'est exigible. Néanmoins, il faut garder à l'esprit, principalement pour l'interprétation de la gestuelle et la traduction, qu'un aspect subjectif n'est pas totalement absent[1168].

[1164] CR-CPP-BOMIO, art. 77 N 1; HAUSER, SCHWERI, HARTMANN, p. 198; SCHMID, Praxiskommentar, art. 78 N 9 et 11.

[1165] ETRILLARD, p. 48; VOGT, p. 411.

[1166] BÜLLESFELD, p. 32; MCDONALD, p. 78.

[1167] ETRILLARD, p. 48; ILL, p. 166.

[1168] Infra Partie II, Chapitre 3, I, B, 4, b, ii, c, n° 1642 ss; Infra Partie II, Chapitre 3, I, B, 4, b, iii, n° 1658-1659.

c. Le contexte technique de la vidéosurveillance

1440 Le système de vidéosurveillance commande l'usage d'une caméra, d'une ligne de transmission, d'un ou de plusieurs moniteurs/écrans permettant la visualisation des images, et, fréquemment, d'un dispositif d'enregistrement[1169].

1441 La capture de l'image, appelée également l'imagerie, est réalisée par une caméra optique, numérique, radar, etc. Selon la caméra employée, la fluidité des mouvements, la précision de l'image et sa luminosité peuvent varier influant sur les possibilités identificatoires ou d'élucidation des faits.

1442 La transmission permet la visualisation de l'image d'un lieu géographiquement distant de la caméra. Avec l'essor de l'informatique, les moyens de transmission ont largement évolué. Généralement, le signal vidéo – se définissant comme la capture de l'image prise par une caméra identifiée par son adresse IP – transite par le réseau informatique local ou internet à l'aide d'un faisceau laser, d'un réseau électrique, d'un satellite, etc.

1443 L'archivage ou le stockage est une technologie employée dans certains types de systèmes de vidéosurveillance. Corrélativement à la transmission, l'évolution de l'informatique permet de stocker les informations visuelles recueillies à l'aide des caméras sur des disques durs ou des supports amovibles. Il est donc possible de garder – en tout cas un certain temps – les images filmées dans le but de les utiliser.

1444 L'analyse de l'image est la dernière technologie liée à la vidéosurveillance. Le développement de l'informatique a fourni des outils utiles pour exécuter certaines tâches automatiquement et permettre un meilleur rendement, extensivement une performance accrue, de l'exploitation des images filmées. Par exemple, il est actuellement possible de détecter les mouvements pour activer la caméra en *standby*; l'identification des véhicules par leurs plaques minéralogiques ou encore la reconnaissance faciale – technique qui se développe rapidement – sont trois autres possibilités offertes par l'automatisation des systèmes de vidéosurveillances. Il est également possible de flouter automatiquement les visages, voire les personnes dans leur entier, afin de mieux respecter la sphère privée et ne décrypter l'image à l'aide d'une clé spécifique qu'en cas de nécessité. Enfin, l'informatique permet d'effectuer des recherches plus rapides. Ainsi, il est possible d'utiliser des centaines de caméras en obtenant des résultats probants pour élucider une infraction ou identifier un individu.

[1169] BAUSCH, p. 5-6; BÜLLESFELD, p. 6-9; CUSSON, Nouvelles technologies, p. 69-70; KLAUSER, Thèse, p. 106; METILLE, Thèse, p. 47-48; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 6-7.

1445 Grâce aux développements technologiques – numériques, techniques et informatiques – quant à la résolution des images, aux possibilités de zoom net, aux capacités de stockage permettant de conserver les captures sans diminuer la qualité des données et la rapidité des réseaux de transmission, la vidéosurveillance permet aujourd'hui de traiter un grand nombre d'images de haute qualité en quelques minutes seulement.

1446 Conséquemment, l'imagerie étant plus nombreuse, claire, précise et balayant une zone géographique plus importante, les préoccupations quant au respect de la sphère privée se sont accrues.

1447 Pour limiter la peur du "Big Brother", une société suisse – EMITALL Surveillance SA – a mis au point un système de vidéosurveillance dite "intelligente"[1170]. Sur la base des recherches effectuées par des chercheurs de l'EPFL, la société EMITALL a créé un logiciel spécifique s'intégrant dans les plates-formes de vidéosurveillance même déjà existantes. Cette technologie permet la détection automatique des faits et gestes filmés et brouille immédiatement l'image mobile avant qu'elle ne soit enregistrée. Ainsi, les visages, la peau, les plaques d'immatriculation sont floutés, mais les objets et locaux immobiles restent nets. Lorsque les données visuelles sont enregistrées, les caractéristiques ou les biens pouvant identifier des personnes ne sont plus reconnaissables garantissant ainsi l'anonymat de ces dernières ainsi qu'un meilleur respect de la sphère privée, principalement grâce à la proportionnalité de l'atteinte. En cas de nécessité – suspicion d'actes délictueux, par exemple –, le processus de brouillage est réversible à l'aide d'une clé d'encryptage ou de déchiffrement que seules les personnes autorisées détiennent.

1448 Quant à l'enregistrement audiovisuel des actes de procédure pénale, techniquement, il n'y a pas de réelle différence. Le système audiovisuel se compose d'une caméra enregistrant le son et l'image, d'un support d'enregistrement ou de stockage et d'un moniteur permettant immédiatement et/ou subséquemment de visualiser les images filmées. En revanche, le logiciel de brouillage n'est pas utilisé puisque la capture des images est employée pour un fait ou un acte de procédure précis après que la direction de la procédure ait apprécié la nécessité de la mesure.

2. Le cadre légal

1449 La démarcation entre la vidéosurveillance dissuasive, préventive ou répressive effectuée par les personnes privées ou les autorités officielles, et celle entre l'observation du domaine secret

[1170] CARNIEL, p. 17; PFPDT, Big Brother.

ou privé et du domaine public, ainsi que l'opposition entre les normes protégeant l'individu et les normes autorisant la vidéosurveillance forment la trame de notre analyse légale quant à la procédure de mise sous surveillance vidéo. En effet, selon le type de vidéosurveillance, la procédure de mise en œuvre diverge.

1450 Sur le plan législatif, nous nous limiterons principalement aux aspects ressortissant aux droits fondamentaux, du droit pénal et de la procédure pénale, ainsi que, brièvement, du droit de la protection des données (LPD et LIPAD/GE).

a. Les droits fondamentaux, les libertés et leur protection

1451 La vidéosurveillance implique de capturer et éventuellement d'enregistrer des images filmées dans la vie de tous les jours. Ainsi, corrélativement aux autres mesures de surveillance, cette technique s'immisce dans la vie privée des individus protégée par la Convention européenne des droits de l'Homme et la Constitution fédérale.

i. La protection des droits fondamentaux et l'atteinte aux libertés causée par la vidéosurveillance

1452 La mise en place et l'exploitation d'un système de surveillance caméra met potentiellement en cause diverses libertés dont la liberté personnelle (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 10 al. 2 Cst), le droit au respect de la sphère privée (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 13 al. 1 Cst), le droit d'être protégé contre l'emploi abusif de ses données personnelles (art. 13 al. 2 Cst), la liberté de réunion (art. 11 CEDH, art. 21 Pacte II et art. 22 Cst), sans oublier le respect de la dignité humaine (art. 3 CEDH, art. 7 Pacte II et art. 7 Cst) qui se conçoit comme un pendant de la liberté personnelle[1171].

[1171] ATF 133 I 77, 79-81 = JdT 2008 I 418, 420-422; ATF 134 I 214, 216; ATF 136 I 87, 112-119 = JdT 2010 I 367, 389-395; ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65-67; CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, §59-60; CourEDH, Affaire *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, 44647/98, § 59; CourEDH, Affaire *Calmanovici c. Roumanie*, arrêt du 1er juillet 2008, 42250/02, § 130; BAUM, n° 18-24; BÜLLESFELD, p. 24-28 et 129-130; DFJP, Rapport vidéosurveillance, p. 25; FLÜCKIGER, p. 207-208; MÉTILLE, Thèse, p. 93-97; MÜLLER, SCHEFER, p. 173; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 49-52; VILLE DE GENÈVE, vidéosurveillance, p. 18.

a) La liberté personnelle

1453 La première liberté mise en péril est la liberté personnelle dans son aspect de garantie de l'intégrité physique, psychique et de la liberté de mouvement.

1454 L'analyse de la mise en cause des droits fondamentaux dans le cadre des empreintes papillaires a mis en exergue la jurisprudence constante du Tribunal fédéral s'agissant du relevé des données personnelles[1172]. Le fait notamment de photographier un prévenu constitue une atteinte à la liberté personnelle touchant à l'intégrité physique et à sa sphère intime[1173]. Datant de plusieurs années, cette jurisprudence doit s'appliquer par analogie à l'évolution technologique et à la création de la prise d'image par une caméra[1174].

1455 Concernant l'intégrité psychique, la doctrine relève que ce droit garantit l'autodétermination individuelle. Ainsi, les individus ont le droit de participer à la vie sociale et d'être à l'abri du regard des autres[1175].

1456 La liberté de mouvement garantit, pour les individus, la protection de la liberté d'aller et venir[1176]. Cette liberté peut être atteinte par une mesure physique – arrestation, détention, etc. – ou par une mesure non privative de liberté au sens strict[1177]. La vidéosurveillance fait partie de cette deuxième catégorie de mesures.

1457 Toute personne désireuse de ne pas être filmée est psychologiquement entravée dans sa liberté de se mouvoir. C'est pourquoi des mesures d'anonymisation des images capturées sont largement préconisées afin de respecter au mieux cette liberté et de permettre aux personne de se mouvoir anonymement[1178].

1458 Enfin, le droit au respect du domicile peut potentiellement être atteint par l'utilisation de la vidéosurveillance[1179]. Ce droit est concrétisé par l'art. 186 CP. Ainsi, tout endroit où une personne mène sa vie privée hors du regard extérieur est considéré comme un domicile.

[1172] ATF 107 Ia 138 = JdT 1982 IV 147; ATF 109 Ia 146; ATF 113 Ia 257; ATF 120 Ia 147 = JdT 1996 IV 61; ATF 137 I 327, 330-331 = JdT 2012 I 125, 128.

[1173] ATF 107 Ia 52, 57; ATF 107 Ia 138, 145 = JdT 1982 IV 147, 151-152; ATF 109 Ia 146, 155; ATF 138 I 256, 262 = JdT 2012 I 102.

[1174] ATF 138 II 346, 356-363 = JdT 2013 I 71, 79-86.

[1175] ATF 90 I 29, 34-36; LEGLER, p. 29; MÜLLER, SCHEFER, p. 142-143; RHINOW, SCHEFER, p. 270-273.

[1176] HÄFELIN, HALLER, KELLER, p. 127-128; MÉTILLE, Thèse, p. 100; MÜLLER, SCHEFER, p. 82 ss; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 49.

[1177] AUBERT, MAHON, art. 10 N 17; AUER, HOTTELIER, MALINVERNI, Vol. II, p. 179-180; MÜLLER, SCHEFER, p. 85.

[1178] Infra Partie II, Chapitre 3, I, B, 4, a, iii, n° 1566.

[1179] MÉTILLE, Thèse, p. 108; METILLE, Surveillance privée, p. 187.

1459 En cas de vidéosurveillance sur domaine privé effectué par une autorité[1180], il ne fait aucun doute que ce droit est atteint dès lors que des images sont capturées dans le cadre de la vie privée d'un individu, et plus spécifiquement dans son lieu d'habitation ou dans tout autre espace privé.

b) Le droit au respect de la sphère privée

1460 Le droit au respect de la sphère privée protège toutes les informations relatives à une personne qui ne sont pas accessibles au public, notamment les données d'identification[1181]. Extensivement, le droit au respect de la sphère privée garantit la protection du domicile contre les ingérences non-consenties[1182].

1461 L'enregistrement d'images de surveillance prises sur la voie publique ou sur des places et la conservation de ces données portent donc atteinte à la sphère privée, si un intérêt à la confidentialité existe, corrélativement aux données signalétiques[1183]. Au contraire, un fait filmé publiquement visible et sans qu'il existe un intérêt à ce qu'il reste secret ne tombe pas sous le coup d'une violation de la sphère privée.

1462 La Commission européenne des droits de l'Homme a en outre précisé qu'un système de surveillance installé dans un lieu public dépourvu de moyen d'enregistrement ne porte pas atteinte à la vie privée. Les données ne peuvent en effet pas être portées à la connaissance du public et les observateurs des images ne voient rien de plus que ce qu'ils auraient obtenu par une présence sur place[1184].

1463 Relevons encore que, malgré l'évolution technologique permettant de visualiser une multitude de caméras et la détection automatique par un programme informatique des événements, la jurisprudence précitée de la Cour européenne reste d'actualité.

[1180] Infra Partie II, Chapitre 3, I, B, 2, c, ii, a) et c), n° 1529 ss et 1547 ss.

[1181] ATF 124 I 34, 36-37; ATF 124 I 85, 87 = JdT 2001 I 318, 319-320; ATF 137 II 371, 380-381.

[1182] AUER, FLÜCKIGER, p. 926; GOLDSCHMID, Überwachung, p. 21-22; MÜLLER, SCHEFER, p. 195-196.

[1183] ATF 133 I 77, 80-81 = JdT 2008 I 418, 421-422; ATF 136 I 87, 101 = JdT 2010 I 367, 379; CourEDH, Affaire *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, 44647/98, § 57-59.

[1184] ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65-67; CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 59-60; CourEDH, Affaire *Calmanovici c. Roumanie*, arrêt du 1er juillet 2008, 42250/02, § 130.

c) Le droit d'être protégé contre l'emploi abusif de ses données personnelles

1464 Le droit à l'autodétermination informationnelle protège les individus contre l'emploi abusif des données personnelles et permet à tout un chacun de se déterminer sur l'utilisation de celles-ci[1185].

1465 Dans certains cas, notamment lorsque les images ne sont pas brouillées ou que la résolution est suffisante, la vidéosurveillance enregistrée ou non capte des images concernant une ou des personnes identifiées ou identifiables[1186]. Il s'agit par conséquent de données personnelles (art. 3 let. a LPD et art. 4 let. a LIPAD/GE) étant précisé qu'elles peuvent être qualifiées de données sensibles (art. 3 let. c LPD art. 4 let. b ch. 2 LIPAD/GE) dans la mesure où elles révèlent la race, l'appartenance religieuse ou politique, etc.

1466 L'utilisation d'un système de vidéosurveillance n'est pas, en tant que tel, interdit. Néanmoins, le droit d'être protégé contre l'emploi abusif des données personnelles impose d'établir des conditions strictes réglementant l'enregistrement, le stockage et/ou l'utilisation des images capturées.

d) La liberté de réunion

1467 La liberté de réunion est le droit de toute personne de se rassembler avec d'autres. Elle garantit l'organisation, la participation ou la non-participation à une réunion, soit à un rassemblement pacifique de plusieurs personnes, de durée limitée, dans un lieu déterminé et dans le but d'échanger des idées ou des opinions[1187].

1468 Corrélativement à ce qui prévaut pour la liberté de mouvement, la vidéosurveillance n'atteint pas physiquement à la liberté de réunion, mais pose une barrière psychologique à toute personne désireuse de ne pas être filmée[1188]. En outre, il n'est pas impossible que la pratique de la surveillance caméra puisse dissuader des organisateurs de convoquer des personnes à une réunion ou qu'elle conduise à assimiler un simple passant à un participant.

[1185] AUER, FLÜCKIGER, p. 933; BONDALLAZ, protection des personnes, p. 70 ss; DSG-BELSER, p. 361 ss; MEIER P., p. 65; MÜLLER, SCHEFER, p. 166 ss; ROSENTHAL, JÖHRI, art. 1 N 5.

[1186] ATF 133 I 77, 80-81 = JdT 2008 I 418, 421-422; ATF 136 I 87, 114-115 = JdT 2010 I 367, 391-392; ATF 138 II 346, 352 = JdT 2013 I 71, 75-76; BAERISWYL, Videoüberwachung, p. 26; PFPDT, Rapport 2003/2004, p. 36; OFJ, avis du 25 juin 1991, p. 165.

[1187] ATF 117 Ia 472, 478-479 = JdT 1993 IV 192; ATF 127 I 164, 168; ATF 132 I 256, 258; AUER, HOTTELIER, MALINVERNI, Vol. II, p. 330-331; GRISEL E., p. 170; Message, Constitution, p. 168; MÜLLER, SCHEFER, p. 578 ss.

[1188] SCHWEGLER, p. 63.

e) La dignité humaine

1469 La dignité humaine instaure comme principe directeur de l'activité étatique que toute personne a le droit d'être traitée de manière humaine et non dégradante[1189].

1470 Ce principe a une importance toute particulière dans le cadre de la procédure pénale, notamment au vu des moyens invasifs de contrainte que l'autorité pénale peut employer[1190]. C'est d'ailleurs pour cette raison que le législateur a consacré expressément le respect de la dignité humaine à l'art. 3 CPP.

1471 Un usage abusif et/ou erroné de la vidéosurveillance peut engendrer une déshumanisation de l'être et, par conséquent, peut nuire au respect de la dignité humaine.

ii. La restriction admissible des droits fondamentaux touchés par la vidéosurveillance

1472 Les droits fondamentaux déploient en premier lieu leurs effets dans la relation verticale entre les autorités et les individus ainsi qu'entre les organismes privés assumant une charge de l'Etat et les particuliers (art. 35 al. 2 Cst)[1191]. Il n'est cependant pas exclu qu'ils soient concernés indirectement entre particuliers, puisque l'Etat a une obligation positive d'adopter des législations imposant leur respect[1192].

1473 Dans le cadre de la vidéosurveillance privée ou étatique, la capture, l'enregistrement, la conservation et le traitement des images créent des atteintes aux droits fondamentaux, ce d'autant que les personnes sont identifiables.

1474 Selon le type de système de surveillance caméra, la nature et l'intensité de l'atteinte varient.

1475 La Cour européenne des droits de l'Homme a déclaré que la vidéosurveillance simple des lieux publics ou accessibles au public sans enregistrement est similaire à une simple

---

[1189] ATF 127 I 6, 13-14; ATF 132 I 49, 55; Message, Constitution, p. 141.

[1190] Message, CPP, p. 1104.

[1191] CourEDH, Affaire *Jäggi c. Suisse*, arrêt du 13 juillet 2006, 58757/00, § 33; CourEDH, Affaire *Calmanovici c. Roumanie*, arrêt du 1er juillet 2008, 42250/02, § 130 ; AUER, HOTTELIER, MALINVERNI, Vol. II, p. 55-68; BELSER, WALDMANN, MOLINARI, p. 108-109.

[1192] ATF 130 III 28, 32; CourEDH, Affaire *Botta c. Italie*, arrêt du 24 février 1998, 21439/93, § 33; CourEDH, Affaire *Jäggi c. Suisse*, arrêt du 13 juillet 2006, 58757/00, § 33; GRISEL E., p. 14-15; MONNIER, Droit d'accès, p. 106-110.

observation. Elle n'atteint donc ni à la liberté personnelle, ni à la sphère privée, ni à la maîtrise informationnelle[1193]. Nonobstant cette jurisprudence, la doctrine suisse soutient qu'une atteinte légère à la sphère privée existe. A l'appui de cette affirmation, elle constate que, contrairement à l'observation, la surveillance est soutenue par une technologie automatisée et est alors plus invasive.

1476 En cas d'enregistrement avec traitement et archivage des images, le droit à la vie privée et à l'autodétermination informationnelle sont atteints[1194], étant précisé que la gravité de l'atteinte est étroitement liée au temps de conservation et à la qualité technologique de l'imagerie[1195]. Ainsi, l'atteinte est qualifiée de légère quand une vidéosurveillance avec enregistrement simple suivi d'un effacement après une brève période est employée, et elle s'aggrave si le dispositif caméra permet un zoom ou filme en haute définition[1196].

1477 Quant à la vidéosurveillance accompagnée d'un enregistrement et d'un traitement informatisé, l'atteinte s'accentue. Elle est considérée comme grave.

1478 L'atteinte à certains droits fondamentaux listés étant avérée, la vidéosurveillance est conforme à la Convention des droits de l'Homme et à la Constitution fédérale (art. 8 § 2 CEDH et art. 36 Cst) si elle se fonde sur une base légale, est nécessaire à l'intérêt public ou à la protection des droits fondamentaux d'autrui et ne viole pas l'essence des droits fondamentaux[1197].

1479 Relevons que plus la liberté ou le droit fondamental est restreint, plus la base légale doit être précise[1198].

1480 Ainsi, la permanence d'une vidéosurveillance dissuasive, la conservation durant une longue durée des enregistrements, l'analyse et/ou le traitement à titre répressif des images, la qualité des données recueillies dites sensibles (art. 3 let. c ch. 2 LPD et art. 4 let. b ch. 2

[1193] ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, 63737/00, § 38 et 40; CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 44; LÉVY V., p. 203.

[1194] ATF 133 I 77, 85 = JdT 2008 I 418, 426; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65-67; CourEDH, Affaire *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, 63737/00, § 38; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 64-65; AUER, FLÜCKIGER, p. 925; DSG-WALDMANN, BICKEL, p. 719-721 et 852 ; MEIER P., p. 232-233;.

[1195] ATF 131 I 272 = TF 1P.570/2004 du 3 mai 2005, c. 6.2 (non publié).

[1196] DSG-WALDMANN, BICKEL, p. 719-721; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 56.

[1197] BAERISWYL, Videoüberwachung, p. 26; HÄFELIN, HALLER, KELLER, p. 93 ss; RHINOW, SCHEFER, p. 199-207.

[1198] ATF 128 I 327, 341 = JdT 2003 I 309, 321; ATF 131 II 271, 278 = JdT 2006 I 678, 681; AUER, HOTTELIER, MALINVERNI, Vol. II, p. 88; GRISEL E., p. 24-25.

LIPAD/GE) et la configuration technique et organisationnelle du système de surveillance comportant un enregistrement avec conservation constituent une atteinte grave aux droits fondamentaux et commandent donc une loi au sens formel[1199].

1481 En droit fédéral et cantonal, la vidéosurveillance dissuasive est réglementée par des normes spécifiques morcelées dans diverses lois et traitées de manière différente[1200]. A lecture de ces lois, si certaines semblent respecter la forme demandée – loi au sens formel – d'autres demandent quelques adaptations ou précisions[1201].

1482 En ce qui concerne le canton de Genève, un projet de loi spécifique à la vidéosurveillance dans son ensemble avait d'ailleurs été déposé[1202]. Cette norme spécifique devait pallier les déficiences liées à la loi sur la police (LPol/GE) et à la généralité de la norme sur la protection des données (LIPAD/GE). En outre, elle devait servir de base légale adéquate et suffisamment précise pour permettre à la police d'employer à titre préventif la vidéosurveillance. Ce projet a été retiré par le Parti démocrate chrétien, en date du 14 décembre 2014, alors qu'il se trouvait en suspens depuis la fin de l'année 2009[1203]. Les raisons de ce retrait ne sont pas connues. Ainsi, à ce jour, la surveillance préventive qui n'entrerait pas dans le champ d'application de la LIPAD/GE (art. 2 et 42 LIPAD) au moyen de caméras est impossible à Genève faute de base légale suffisante. Cette situation devrait évoluer si la nLPol/GE entre en vigueur, notamment avec la modification de l'art. 56 al. 1 nLPol/GE.

1483 Quant à la vidéosurveillance invasive, des règles claires et précises sont fixées par la procédure pénale. La condition de l'existence d'une base légale suffisante ne pose donc aucun problème.

[1199] BSK-DSG-BELSER, art. 3 N 19; BSK-DSG-GABOR, art. 3, N 47-61; BSK-DSG-MAURER-LAMBROU, STEINER, art. 4 N 37-40b; BÜLLESFELD, p. 129; FLÜCKIGER, p. 214; Message, LPD, 473.

[1200] Notamment: Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale (OSF), RS 120.72; Code de procédure pénale suisse du 5 octobre 2007 (CPP), RS 312.00; Loi fédérale du 20 décembre 1957 sur les chemins de fer (LCdF), RS 742.101; Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics (OVid-TP), RS 742.147.2; Loi du 20 mars 2009 sur le transport de voyageurs (LTV), RS 745.1; Ordonnance du 24 septembre 2004 sur les jeux de hasard et les maisons de jeu (Ordonnance sur les maisons de jeu, OLMJ), RS 935.521; Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD), RS/GE A 2 08; Loi du 26 juin 2008 sur les manifestations sur le domaine public (LMDPu/GE), RS/GE F 3 10.

[1201] DFJP, Rapport vidéosurveillance, p. 26; FLÜCKIGER, p. 216.

[1202] Projet de loi sur la vidéosurveillance – PL 10545 déposé le 17 septembre 2009.

[1203] Informations disponibles sur le site de la Commission judiciaire et de police : http://ge.ch/grandconseil/memorial/seances [consulté le 08.05.2016].

1484 Le Tribunal fédéral a admis que la garantie de l'ordre public, la sécurité, la prévention d'actes délictuels futurs et la poursuite d'actes délictuels commis est d'intérêt public[1204]. La vidéosurveillance étant utilisée à titre préventif et répressif pour possiblement identifier un ou des auteurs d'infraction, présenter les faits et circonstances de commission ainsi que pour diminuer le sentiment d'insécurité de la population ou des particuliers, il ne fait nul doute que la condition d'intérêt public prépondérant et/ou la protection des libertés ou droit fondamentaux d'autrui est donnée.

1485 Quant à la proportionnalité, l'aptitude est vraisemblablement donnée. La vidéosurveillance fournit un moyen d'investigation et de preuve efficace – vidéosurveillance invasive – et la présence des caméras vidéo peuvent inciter une personne à ne pas commettre un acte délictuel – vidéosurveillance dissuasive – de peur d'être identifiée et poursuivie[1205]. Malgré le fait que l'efficacité du système de surveillance caméra ne soit pas objectivement démontrée, il n'est pas possible d'emblée de considérer la vidéosurveillance comme inefficace, ce qui est suffisant aux fins de l'aptitude de la mesure.

1486 La subsidiarité et la nécessité commandent qu'un moyen alternatif, moins invasif, soit utilisé s'il permet d'atteindre le but recherché, que seule la zone absolument nécessaire doit être surveillée et que les caméras doivent être activées seulement durant le temps nécessaire. Ainsi, la vidéosurveillance n'est acceptable qu'à titre subsidiaire et doit se limiter aux endroits problématiques ou à une certaine catégorie de personnes.

1487 Quant à la pesée des intérêts, il est difficilement envisageable de prédire la décision d'un juge à savoir si oui ou non l'intérêt à la prévention ou à la répression est prépondérant face aux intérêts des particuliers dont les libertés fondamentales sont restreintes par la vidéosurveillance. Le respect de la proportionnalité au sens strict va dépendre du système technique de surveillance mis en place, de la gravité de l'atteinte, du facteur temporel de la conservation des images – le Tribunal fédéral a reconnu comme proportionnée la conservation durant cent jours[1206] – et du type de vidéosurveillance – par exemple, la vidéosurveillance invasive n'atteint qu'à la liberté d'un individu soupçonné, alors que la vidéosurveillance dissuasive touche un grand nombre de personnes.

[1204] ATF 120 Ia 147, 151 = JdT 1996 IV 61, 61; ATF 131 I 272, 275; TF 6B_536/2009 du 12 novembre 2009, c 3. 7 = SJ 2010 I 394, 398.

[1205] ATF 120 Ia 147, 151 = JdT 1996 IV 61, 61; ATF 131 I 272, 275; ATF 133 I 77, 83-88 = JdT 2007 I 591, 597-601; ATF 136 I 87, 101-104 = JdT 2010 I 367, 379-382; TF 6B_536/2009 du 12 novembre 2009, c 3. 7 = SJ 2010 I 394, 398.

[1206] ATF 133 I 77, 83-88 = JdT 2007 I 591, 597-601; ATF 136 I 87, 101-104 = JdT 2010 I 367, 379-382.

1488 En conséquence, rien ne s'oppose d'office à l'utilisation de la vidéosurveillance sur domaine public ou privé.

b. La protection du Code pénal

1489 Dans le cadre de notre recherche, l'analyse légale de la vidéosurveillance par les particuliers et par les autorités fédérales ou cantonales est interdépendante du domaine filmé (privé, secret ou publique).

1490 Pénalement, l'art. 179*quater* CP interdit à toute personne ou autorité d'observer, à l'aide d'un appareil de prise de vues, ou de fixer sur un porteur d'images des faits relevant du domaine secret ou du domaine privé et qui ne peuvent pas être perçus par tout un chacun[1207]. Cette infraction réprime donc, notamment, la vidéosurveillance qui capte des faits – compromettants ou non – connus d'un cercle restreint de personnes, qui ne sont pas accessibles et que la personne souhaite légitimement garder secrets – domaine secret –, ou encore, des faits qui ne peuvent pas être perçus par n'importe qui – domaine privé – protégeant ainsi le lieu où les gens se sentent à l'abri des regards[1208].

1491 Même si la jurisprudence n'a jamais tranché la question de savoir si la notion de domaine privé de l'art. 179*quater* CP permettait de protéger des faits relevant de la vie privée et qui se dérouleraient en public, une partie de la doctrine est d'avis de se limiter à la protection du lieu à l'abri des regards[1209]. En revanche, elle réfute la possibilité d'étendre la protection aux faits de la vie privée qui se déroulent en public. Ainsi, l'infraction de l'art. 179*quater* CP ne réprime pas la surveillance du domaine public ou accessible au public[1210]. Nonobstant l'atypicité pénale, ce type de vidéosurveillance n'est pas sans limite puisqu'elle est attentatoire aux droits fondamentaux.

1492 Au surplus, corrélativement à la surveillance des télécommunications[1211], la vidéosurveillance est un moyen d'investigation et de preuve utile à la procédure pénale. Par conséquent, l'art. 179*octies* autorise les autorités pénales à recourir à ce moyen de surveillance dans les limites

---

[1207] ATF 117 IV 31, 34; ATF 118 IV 41, 46 = JdT 1994 IV 79, 81; ATF 137 I 327, 335-336 = JdT 2011 I 125, 132-133; NOLL, p. 95; STRATENWERTH, WOHLERS, art. 179*quater* N 1-2.

[1208] ATF 117 IV 31, 33; ATF 118 IV 41, 45-46 = JdT 1994 IV 79, 81; ATF 137 I 327, 335-336 = JdT 2011 I 125, 132-133.

[1209] COQUOZ, p. 659-660; STRATENWERTH, JENNY, BOMMER, p. 275-276.

[1210] NOLL, p. 95; RIKLIN, Strafprozessordnung, art. 280 N 3; TRECHSEL, Kurzkommentar, art. 179*quater* N 3.

[1211] Supra Partie II, Chapitre 3, I, A, 2, b, ii, n° 1136 ss; Supra Partie II, Chapitre 3, I, A, 2, d, n° 1226 ss.

prévues par la loi. La vidéosurveillance peut également se justifier par la légitime défense, l'état de nécessité ou la *Beweisnotstand*.

c. Les normes fédérales et cantonales élémentaires à la vidéosurveillance

1493 Dès lors qu'une personne est identifiable, la capture d'une image par une caméra suppose le traitement de ses données personnelles au sens de la LPD ou de la LIPAD/GE [1212], étant précisé que les principes généraux de protection des données (conformité au but, communication, accès aux données, durée limite de conservation, etc.) doivent être respectés. Ces deux lois de nature générale et abstraite sur la protection des données personnelles s'appliquent à tout traitement de données liées à la personnalité de l'auteur, soit notamment au traitement des images issues de la vidéosurveillance[1213].

1494 Concernant la vidéosurveillance effectuée dans le cadre d'une procédure pénale pendante, la LPD et la LIPAD/GE ne sont pas applicables (art. 2 al. 2 let. c LPD et art. 42 al. 1 let. a LIPAD/GE)[1214]. En effet, les normes spécifiques de la procédure pénale le sont (art. 280 ss CPP).

1495 Relevons que pour exercer certaines tâches – maintien de la sécurité intérieure (LMSI)[1215], surveillance des douanes (LD et l'ordonnance du 4 avril 2007)[1216], etc. – ou dans des cas particuliers – exploitation d'un système de surveillance dans les transports publics (LCdF[1217], OVid-TP[1218], LTV[1219]) ou dans les maisons de jeu (OLMJ[1220]), etc. – des réglementations spécifiques sont édictées.

[1212] BSK-DSG-BELSER, art. 3 N 5-6; BSK-DSG-GABOR, art. 3, N 6-13; DSG-WALDMANN, BICKEL, p. 719-721 et 852; MEIER P., p. 197-199.

[1213] Message, LPD, p. 452.

[1214] Supra Partie I, Chapitre 2, II, A, 2, b, i, n° 244; Supra Partie I, Chapitre 2, II, B, 2, n° 272.

[1215] Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI), RS 120.

[1216] Loi fédérale du 18 mars 2005 sur les douanes (LD), RS 631.0; Ordonnance du 4 avril 2007 régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'Administration fédérale des douanes, RS 631.053.

[1217] Loi fédérale du 20 décembre 1957 sur les chemins de fer (LCdF), RS 742.101.

[1218] Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics (OVid-TP), RS 742.147.2.

[1219] Loi du 20 mars 2009 sur le transport de voyageurs (LTV), RS 745.1.

[1220] Ordonnance du 24 septembre 2004 sur les jeux de hasard et les maisons de jeu (Ordonnance sur les maisons de jeu, OLMJ), RS 935.521.

1496 En outre, en ce qui concerne la vidéosurveillance effectuée par les particuliers, le préposé fédéral à la protection des données et à la transparence a complété le cadre dans lequel l'usage d'un système caméra est acceptable[1221]. Ce texte fait office de *soft law*.

i. La vidéosurveillance effectuée par les particuliers

1497 La vidéosurveillance dite privée est installée et utilisée par des individus agissant à titre personnel, pour le compte de personnes morales ou en tant qu'entreprise de sécurité privée[1222]. Les acteurs de cette surveillance sont divers et variés, il peut s'agir de simples particuliers désireux de protéger leur domicile, de banques, d'entreprises, de magasins, de centres commerciaux, d'assurances pour détecter les fraudes, etc.

1498 Aucune loi *ad hoc* ne règle la collecte d'images par des personnes privées. Par conséquent, ce type de vidéosurveillance relève du droit de la protection de la personnalité et de la sphère privée. L'art. 28 CC, les principes généraux de la LPD et l'art. 179*quater* CP complétés par des normes spécifiques – par exemple, l'art. 328 et 328*b* CO sur le droit du travail – sont les dispositions principales qui encadrent l'utilisation de la vidéosurveillance par les particuliers.

a) L'art. 28 CC

1499 En droit civil, le fondement de la protection de la personnalité dans les rapports entre particuliers est édicté à l'art. 28 CC. Cette disposition prévoit que tout acte d'un tiers causant un trouble à un ou plusieurs intérêts personnels est en principe illicite.

1500 La protection issue de l'art. 28 CC s'étend à la vie intime et à la vie privée des individus. Les événements ressortant de la vie publique ne sont en revanche pas protégés.

1501 Lors de l'exercice de la vidéosurveillance par des particuliers, il n'est pas impossible que certaines images montrent un fait ou un geste soustrait à la connaissance de tout un chacun ou partagé avec un nombre restreint d'autres personnes étroitement liées. En règle générale, cette surveillance vidéo est donc illicite.

[1221] PFPDT, Vidéosurveillance.

[1222] LEGLER, p. 186-190; METILLE, Surveillance privée, p. 181-182.

1502 Cependant, l'alinéa 2 de l'art. 28 CC nuance la portée de la protection, si l'auteur peut invoquer un motif justificatif – consentement du lésé, intérêt privé ou public prépondérant[1223] ou une loi – la présomption d'illicéité est renversée. Ainsi, dans certaines circonstances, la capture de données par les personnes privées au moyen d'un système de vidéosurveillance est admissible[1224].

b) L'art. 179quater CP

1503 Pénalement, les exploitants d'un système de vidéosurveillance privée doivent s'assurer que l'art. 179*quater* CP n'est pas violé par une atteinte à la sphère privée et intime de l'individu filmé lors de l'acquisition et de l'exploitation des images relevées[1225].

1504 Le positionnement d'une caméra de surveillance est alors essentiel. Il n'est pas concevable que le champ de vision s'étende à l'entourage immédiat ou à l'intérieur du domicile d'un tiers[1226], voire à des locaux relevant du domaine intime comme les toilettes[1227].

1505 Si le dessein de l'auteur est de filmer un acte relevant de la sphère privée ou intime à des fins probatoire par exemple, il doit se prémunir d'un motif justificatif[1228].

c) Les principes généraux de la LPD et l'applicabilité des art. 12 ss LPD

1506 Bien que les images ne sont pas toujours destinées à être analysées ni conservées pour une durée illimitée, elles peuvent porter atteinte au droit de la personnalité[1229].

1507 L'utilisation par des particuliers de la vidéosurveillance – filmant le domaine privé ou accessible au public – aux fins de se protéger ou de prévenir des actes de vandalisme est soumise à la loi fédérale sur la protection des données dans l'hypothèse où les images se rapportent à des personnes identifiées ou identifiables (art. 2 al. 1 let. a et 3 let. a LPD). Cette loi contient des dispositions pénales et consacre les principes généraux à respecter lors de

[1223] Infra Partie II, Chapitre 3, I, B, 2, c, ii, n° 1531, 1537, 1545 ss et 1553.

[1224] MEIER P., p. 509.

[1225] BAUM, n° 5 et 18-24; CORBOZ, p. 610-618; LEGLER, p. 137.

[1226] ATF 118 IV 41, 48-49 = JdT 1994 IV 84; ATF 137 I 327, 335-336 = JdT 2012 I 125, 132-133.

[1227] LEGLER, p. 189.

[1228] Supra Partie II, Chapitre 3, I, A, 2, b, ii, n° 1138.

[1229] LÉVY V., p. 202.

l'exploitation d'une surveillance caméra, notamment: la licéité du traitement, la proportionnalité, la bonne foi, la finalité et la sécurité technique[1230].

1. Le principe de licéité (art. 4 al. 1 LPD)

1508 En principe, la collecte des données est illicite sous réserve de l'assentiment de l'ayant-droit, d'un intérêt privé ou public prépondérant ou de la loi autorisant le comportement (art. 4 al. 1, 12 et 13 LPD)[1231] étant précisé que le traitement des données issues de la surveillance du domaine accessible au public ne porte pas atteinte à la personnalité si la personne concernée a rendu les données accessibles à tout un chacun[1232] et ne s'est pas opposée formellement au traitement (art. 12 al. 3 LPD).

1509 Afin de dissuader les comportements indésirables, d'assurer la conservation de preuve ou d'en obtenir, les particuliers peuvent donc, dans certaines circonstances, recourir à la vidéosurveillance dissuasive ou invasive sur domaine privé ou public.

1510 Le plus souvent, surtout sur le domaine accessible au public, le consentement est la règle pour justifier la surveillance caméra par les particuliers[1233]. En pratique, le simple fait de se promener sur la zone surveillée n'est pas suffisant pour reconnaître l'accord du lésé, ni déclarer que les données sont accessibles à tout un chacun. En revanche, si une personne pénètre dans un lieu signalé comme surveillé par des caméras, il est admissible de présumer que le lésé a donné librement son consentement avant la capture des images et que par conséquent l'enregistrement et le traitement de ses données sont admissibles[1234]. Relevons néanmoins qu'en cas de profil de la personnalité ou de données sensibles, le consentement doit être explicite (art. 4 al. 4 *in fine* LPD).

1511 Pour s'assurer de la licéité, le préposé fédéral à la protection des données et à la transparence préconise néanmoins de toujours avoir un intérêt privé ou public prépondérant. Cet intérêt est largement reconnu lorsqu'il s'agit d'installer un système de surveillance à des fins de sécurité[1235].

[1230] A ce sujet: BONDALLAZ, protection des personnes, p. 164-166; BSK-DSG-RAMPINI, art. 12 N 9; MEIER P., p. 260-308.

[1231] BONDALLAZ, protection des personnes, p. 162; BSK-DSG-RAMPINI, art. 12 N 9 et art. 13 N 3 ss; METILLE, Surveillance privée, p. 187-188.

[1232] BSK-DSG-RAMPINI, art. 12 N 16; MEIER P., p. 524-526.

[1233] BSK-DSG-RAMPINI, art. 13 N 3.

[1234] AUER, FLÜCKIGER, p. 927; BSK-DSG-RAMPINI, art. 13 N 4; MEIER P., p. 529; RIKLIN, Medialex 2007, p. 55-56.

[1235] PFPDT, Vidéosurveillance.

1512 Lorsque la loi sert de motif justificatif, le législateur a procédé à une pesée des intérêts et ordonne ou permet le traitement des données dans une loi au sens formel ou matériel[1236]. Ce motif justificatif n'est invocable que pour le but prévu par la loi et non pas de manière générale[1237].

1513 Pour exemple, le Tribunal fédéral a reconnu comme licite les images d'une personne touchant des indemnités AI prises par un détective privé engagé par une assurance afin de déterminer si l'assuré percevait indûment des prestations. La Cour a constaté que les art. 28 al. 2 et 43 LPGA ainsi que l'art. 59 al. 5 LAI sont des bases légales suffisantes pour autoriser la surveillance des personnes assurées[1238], malgré le fait que la vidéosurveillance ne soit pas explicitée et que la densité normative exigée en cas de capture et d'enregistrement d'image fait quelque peu défaut.

1514 Quant à l'intérêt prépondérant, le traitement des données de manière globale ou partielle peut être autorisé. Il suffit que l'intérêt aux traitements des données prédomine sur l'intérêt de la personne à ne pas être blessée dans sa personnalité, pesée devant se réaliser à la lumière du cas d'espèce[1239].

1515 Pour déterminer quels intérêts peuvent entrer en ligne de compte pour justifier la vidéosurveillance, le juge peut s'appuyer sur l'art. 13 al. 2 LPD. Cette disposition permet en outre aux personnes concernées par la capture des images et aux auteurs du traitement de prévoir dans quelles circonstances un traitement de données peut être licite. A la lumière de l'atteinte pouvant être causée par le traitement – touchant l'un des droits fondamentaux le plus important de l'individu –, la prévisibilité juridique accentuée par l'art. 13 al. 2 LPD est essentielle.

2. Le principe de proportionnalité (art. 4 al. 2 LPD)

1516 La vidéosurveillance doit être effectuée conformément au principe de proportionnalité. A cet égard, elle doit être un moyen adéquat de réaliser le but poursuivi, être subsidiaire et l'atteinte à la sphère privée doit être proportionnée par rapport au but visé.

[1236] ATF 140 I 381; DSG-EPINEY, p. 518-519; BSK-DSG-RAMPINI, art. 13 N 16; MEIER P., p. 260 et 530-531.

[1237] BSK-DSG-MAURER-LAMBROU, STEINER, art. 4 N 13-14; BSK-DSG-RAMPINI, art. 13 N 15 ss; MEIER P., p. 523-524.

[1238] ATF 137 I 327, 331 = JdT 2012 I 125, 128.

[1239] ATF 97 II 97, 105-106 = JdT 1972 I 242, 249-250; ATF 126 III 305, 306-307 = JdT 2001 I 34, 36-37; BSK-DSG-RAMPINI, art. 13 N 25-26; MEIER P., p. 532 ss; ROSENTHAL, JÖHRI, art. 12 N 36.

1517 L'adéquation doit se concevoir dans chaque cas concret. Le préposé à la protection des données et à la transparence reconnaît notamment comme adéquate l'utilisation d'un système de caméra pour réaliser le but de sécurité, notamment pour la protection contre les atteintes aux personnes ou aux biens[1240]. Il est également important que les caméras ne captent que les images propres à atteindre le but désiré. Il n'est par exemple pas concevable qu'un système de vidéosurveillance installé pour sécuriser l'entrée d'une maison filme les allées et venues sur la chaussée du voisin.

1518 L'apposition de verrous supplémentaires, la pose d'une porte sécurisée, l'installation d'un système d'alarme, etc. doivent s'avérer irréalisables ou insuffisantes. Dans l'hypothèse inverse, l'exploitation de la vidéosurveillance ne respecte pas le principe de subsidiarité et est déclarée disproportionnée.

1519 D'après la jurisprudence, il faut différencier la surveillance sur domaine accessible au public de l'espace privé pour la pesée des intérêts[1241].

1520 Les images captées sur domaine public ne constitueraient qu'une atteinte légère aux droits de la personnalité[1242]. Nous nous accordons à reconnaître que, comparativement à la surveillance d'un lieu intime, les images filmées sur domaine public ou accessible à tout un chacun constituent une atteinte moins grave que celles du domaine privé ou secret. Néanmoins, il faut tempérer à notre sens la décision de la Cour, l'épanouissement personnel, la vie privée et les relations sociales doivent être protégées de manière adéquate même sur domaine public[1243], ce d'autant que ledit domaine n'empêche pas que des faits relevant du domaine secret de l'individu soient capturés.

1521 Quant à l'atteinte causée par l'enregistrement vidéo de faits d'autrui se déroulant sur domaine privé, elle peut être d'intensité très élevée, puisque les zones spatiales de vie sont le centre de l'épanouissement et du développement personnel. C'est d'ailleurs pour cette raison que le droit au respect du domicile renforce la protection de l'autodétermination informationnelle.

1522 En d'autres termes, les images captées sur domaine public engendrent une atteinte plus ou moins grave aux droits de la personnalité dépendamment du type de faits filmés, et celles

[1240] PFPDT, Vidéosurveillance.

[1241] ATF 132 V 241, 242; ATF 135 I 169, 171 et 173-174 = JdT 2010 I 191, 193 et 195-196; ATF 136 III 410, 413-414, 415 et 420-421.

[1242] ATF 132 V 241, 242; ATF 135 I 169, 171 et 173-174 = JdT 2010 I 191, 193 et 195-196; ATF 136 III 410, 413-414, 415 et 420-421.

[1243] MÜLLER, n° 21.

prises sur domaine privé créent une atteinte considérée comme grave, même lorsqu'elles révèlent uniquement des faits dits "de la vie quotidienne" ou "de la routine"[1244]. Il faut, par conséquent, mettre en balance l'intensité de l'atteinte causée avec le but visé pour déterminer au cas par cas si oui ou non l'exploitation d'un système de surveillance est proportionnée.

1523 Aux fins de la proportionnalité, il est également utile de limiter le nombre de personnes qui ont accès aux images diffusées en direct ou enregistrées, et de vérifier si une surveillance en direct ou avec enregistrement est nécessaire pour atteindre le but recherché. Dans l'hypothèse où les captures sont enregistrées, il est impératif qu'après un certain délai les données soient effacées. Pour le préposé à la protection des données, un délai de vingt-quatre heures est suffisant lorsque la finalité de la vidéosurveillance sert à l'établissement des infractions aux personnes ou aux biens. Néanmoins, un délai plus long n'est pas d'office exclu, ce d'autant si la vidéosurveillance filme un lieu non accessible au public et que le propriétaire est en vacances[1245]. En outre, sur domaine public, la jurisprudence a admis que le délai de conservation peut être de plusieurs jours – en l'espèce de cent jours – si les images peuvent servir dans le cadre d'une procédure pénale[1246].

3. Le principe de bonne foi (art. 4 al. 2 LPD)

1524 Le devoir unilatéral d'informer (art. 14 LPD) impose qu'une indication avertisse la(les) personne(s) concernée(s) de l'existence de la vidéosurveillance, fournisse les coordonnées du responsable du traitement et mentionne le droit d'accès aux images enregistrées.

1525 Il n'existe aucune exigence de forme, l'information peut donc être donnée oralement ou sous la forme écrite selon divers types de support tant qu'elle est visible, lisible et intelligible[1247]. Sans une information correcte et accessible, le principe de bonne foi fait défaut entrainant l'impossibilité de faire valoir son droit d'accès (art. 8 LPD).

4. Le principe de finalité (art. 4 al. 3 LPD)

1526 Le principe de finalité veut que les données enregistrées à l'aide d'un système de caméra ne soient utilisées que dans le cadre du but recherché. Ainsi, l'exploitation d'une

[1244] MÜLLER, n° 26.

[1245] PFPDT, Vidéosurveillance.

[1246] ATF 133 I 77, 83-88 = JdT 2007 I 591, 597-601.

[1247] BSK-DSG-RAMPINI, art. 13 N 3 et 9 ss; WERMELINGER, SCHWERI, n° 21 et n° 25.

vidéosurveillance pour sécuriser et protéger son domicile contre les atteintes aux biens ou aux personnes ne peut s'accompagner de l'utilisation des images sur Internet.

1527 Par conséquent, si la vidéosurveillance est utilisée pour prévenir des infractions, les images capturées ne peuvent servir qu'à dénoncer aux autorités les agissements d'un individu, voire à être utilisées comme moyen de preuve.

5. Le principe de sécurité des données

1528 La sécurité des données impliquent la prise de mesures organisationnelles et techniques. La vidéosurveillance engendrant une atteinte au droit de la personnalité, il est essentiel que le but poursuivi, la finalité et la proportionnalité soient respectés. Si les données sont accessibles à tout un chacun, il ne fait nul doute que les principes précédemment cités ne sont pas remplis.

1529 Il est par conséquent nécessaire que les images ne puissent pas être interceptées par des personnes non autorisées, ce qui implique la mise en place de cryptage ou de ligne réseau sécurisée en cas de transfert des données, étant précisé que plus les images sont conservées longtemps, plus l'atteinte est grave et donc plus les exigences en matière de sécurité sont élevées.

ii. La vidéosurveillance effectuée par les autorités

a) La vidéosurveillance dissuasive du domaine privé ou secret

1530 Le domaine privé échoit au propriétaire du fond qui est alors habilité à filmer sa propriété. Les autorités publiques ne disposent que du seul domaine public entendu dans son sens large, soit tout espace accessible au public[1248].

1531 Le principe de l'inviolabilité du domicile sans l'accord du propriétaire (art. 8 CEDH, art. 17 Pacte II, art. 13 al. 1 Cst et art. 186 CP) interdit aux autorités publiques – fédérales ou cantonales – de surveiller à des fins dissuasives la propriété d'une personne privée ou morale. Le lieu d'habitation, les espaces privés ouverts ou fermés et les lieux provisoires ou

[1248] ATF 136 I 87, 113-114 = JdT 2010 I 367, 390-391.

temporaires comme une chambre d'hôtel sont protégés contre l'intrusion des organes étatiques[1249].

1532 Ainsi, la vidéosurveillance dissuasive ne peut pas être exercée par les collectivités publiques et les organes agissant en leur nom sur domaine privé ou secret à défaut de l'assentiment de l'ayant droit ou d'une base légale spécifique[1250].

b) La vidéosurveillance dissuasive des espaces publics

1533 La vidéosurveillance du domaine public comprend l'espace public – rues, places, parcs, etc. – et le patrimoine administratif – hôpitaux, bâtiments étatiques, parkings en mains publiques, etc.[1251] Elle peut être exercée par une autorité cantonale ou fédérale.

1534 Le cadre juridique dépend étroitement de la qualité de l'autorité qui exerce la vidéosurveillance. Alors que l'art. 28 CC n'est pas applicable puisqu'il s'agit d'une norme de droit privé[1252] – qui règlemente donc les rapports entre particuliers –, la LPD n'encadre que l'activité des organes fédéraux (art. 2 al. 1 let. b LPD) et le droit cantonal s'applique à la surveillance dissuasive exercée par les autorités cantonales.

1. L'exercice de la vidéosurveillance dissuasive par les organes fédéraux

1535 Dans le cadre de la vidéosurveillance dissuasive exercée par les autorités fédérales et leurs organes, la LPD étant applicable, les principes généraux du droit de la protection des données (art. 4 ss LPD) doivent être respectés[1253]. Ils sont complétés par les articles 16 à 25 LPD.

1536 Afin d'éviter toutes redondances, nous nous bornerons à spécifier quelques points précis.

1537 La vidéosurveillance dissuasive du domaine public par les organes fédéraux est interdite sans une base légale (art. 17 al. 1 LPD). La capture des images étant propres à informer l'autorité sur les opinions et/ou activités religieuses, sur la santé, la sphère intime, l'appartenance à une race, etc., les données ainsi recueillies constituent des données sensibles (art. 3 let. c

[1249] MÉTILLE, Thèse, p. 108-109; MÜLLER, SCHEFER, p. 195-196.

[1250] AUER, FLÜCKIGER, p. 926; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 46-47.

[1251] FLÜCKIGER, p. 207; HOTTELIER, SJ 2002, p. 123-126.

[1252] ATF 101 II 177, 185-186 = JdT 1976 I 362, 370-371; ATF 136 III 410, 421.

[1253] Supra Partie II, Chapitre 3, I, B, 2, c, i, c), n° 1508 ss.

LPD), voire peuvent former un profil de la personnalité en étant couplées avec d'autres informations (art. 3 let. d LPD). Il en résulte que les normes spécifiques doivent être de nature formelle (art. 17 al. 2 LPD).

1538 Exceptionnellement, le traitement des profils de la personnalité ou des données sensibles est possible si l'accomplissement d'une tâche définie dans une loi au sens formel l'exige (art. 17 al. 2 let. a LPD), si le Conseil fédéral l'a autorisé (art. 17 al. 2 let. b LPD) ou si l'autorité obtient le consentement de la personne concernée, si elle a rendu les données accessibles ou tout du moins si elle ne s'est pas opposée formellement au traitement (art. 17 al. 2 let. c LPD).

1539 Concernant les hypothèses de la let. c de l'art. 17 al. 2 LPD, la présence dans le champ de vision ne suffit pas[1254]. A la différence de la vidéosurveillance effectuée par les particuliers, le consentement implicite n'est pas satisfaisant puisque nous ne pouvons pas exiger d'un individu de changer de rue ou de place pour ne pas être filmé. En effet, admettre le consentement implicite impliquerait de forcer le consentement et, au fur et à mesure de l'étendue de la vidéosurveillance, à restreindre la liberté de mouvement de manière inadmissible en empêchant la population de se déplacer. C'est pourquoi la doctrine demande que le consentement soit express, volontaire et éclairé[1255].

1540 Au surplus, les principes généraux de la protection des données devant être respectés[1256], dans l'intérêt public à la prévention d'actes délictuels[1257] et à l'identification de leurs auteurs[1258], les organes fédéraux sont en droit d'installer des systèmes de caméra surveillance moyennant l'existence d'une base légale au sens formel et le respect du principe de proportionnalité analysable au cas par cas, notamment en ce qui concerne la durée de conservation qui est dépendante de la finalité de la mesure[1259].

1541 Relevons encore, sans entrer dans les détails, que des normes spécifiques[1260] complètent la réglementation applicable à l'utilisation d'un système de vidéosurveillance. Toutes ces

[1254] Supra Partie II, Chapitre 3, I, B, 2, c, i, c), n° 1509.

[1255] BALLANEGGER, MOJER, art. 17 N 30-33; BSK-DSG-JÖHRI, STUDER, art. 17 N 49-53; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 59.

[1256] Supra Partie II, Chapitre 3, I, B, 2, c, i, c), n° 1508 ss.

[1257] ATF 109 Ia 138, 146-147; ATF 109 Ia 146, 155-156; ATF 120 Ia 147, 151 = JdT 1996 IV 61, 61; ATF 137 I 167, 187-188.

[1258] ATF 109 Ia 138, 146-147; ATF 109 Ia 146, 155-156; ATF 137 I 167, 184-185.

[1259] ATF 133 I 77, 83-88 = JdT 2007 I 591, 597-601; ATF 136 I 87, 116-117 = JdT 2010 I 367, 393-394.

[1260] Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale (OSF), RS 120.72; Ordonnance du 4 avril 2007 régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par

dispositions légales correspondent à des tâches particulières qui doivent être exercées par les organes fédéraux afin de les aider à accomplir leurs devoirs.

2. L'exercice de la vidéosurveillance dissuasive par les autorités cantonales

1542 Sortant du champ d'application de la LPD (art. 2 *a contrario* LPD), la vidéosurveillance dissuasive par les collectivités publiques ou les institutions publiques cantonales ressort du droit cantonal complété de manière supplétive par la LPD (art. 37 al. 1 LPD) et les principes généraux de la protection des données (art. 4 ss LPD par analogie).

1543 A Genève, l'abrogation de la LITAO/GE s'est accompagnée de l'entrée en vigueur de la LIPAD/GE qui instaure une base légale et des conditions spécifiques pour l'installation des systèmes de vidéosurveillance (art. 42 LIPAD/GE)[1261].

1544 L'art. 42 LIPAD/GE se conçoit comme une norme générique qui renforce les dispositions spécifiques éparses[1262] – par exemple, possibilité de filmer les participants à une manifestation (art. 22 aLPol/GE) – qui ne s'appliquent pas à tous les domaines de vidéosurveillance préventive. Ainsi, la LIPAD/GE fournit notamment une base légale suffisante pour toute vidéosurveillance dissuasive ou préventive entrant dans son champ d'application (art. 2 LIPAD/GE).

1545 Dans les grandes lignes, en dehors des tâches de la collectivité publique ou de ses institutions ressortant d'une loi cantonale spéciale, l'art. 42 LIPAD/GE pose la condition de principe à la licéité de l'installation et d'exploitation d'un système de vidéosurveillance.

1546 Ainsi, la création et l'exploitation d'un système de caméra de surveillance doit cumulativement respecter les exigences: d'adéquation, de finalité, d'intérêt public prépondérant, de proportionnalité, de transparence – installation des caméras à des endroits visibles –, d'information – signalisation du système de vidéosurveillance –, de communication

l'Administration fédérale des douanes, RS 631.053; Loi fédérale du 20 décembre 1957 sur les chemins de fer (LCdF), RS 742.101; Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics (OVid-TP), RS 742.147.2; Loi du 20 mars 2009 sur le transport de voyageurs (LTV), RS 745.1; Ordonnance du 24 septembre 2004 sur les jeux de hasard et les maisons de jeu (Ordonnance sur les maisons de jeu, OLMJ), RS 935.521; Ordonnance du DFJP du 24 septembre 2004 sur les systèmes de surveillance et les jeux de hasard (Ordonnance sur les jeux de hasard, OJH), RS 935.521.21; etc.

[1261] Projet de loi du Conseil d'Etat de Genève sur la protection des données personnelles (LPDP) – PL 9870, p. 34.

[1262] Loi du 26 juin 2008 sur les manifestations sur le domaine public (LMDPu/GE), RS/GE F 3 10; Règlement du 31 août 1988 relatif à l'exécution de la loi sur la restauration, le débit de boissons et l'hébergement (RRDBH/GE), RS/GE I 2 21.01; etc.

des données, de leur destruction après un bref délai, en principe de sept jours, et pouvant se porter jusqu'à trois mois en cas d'atteinte avérée aux personnes ou aux biens – et de sécurité afin de protéger les données contre un traitement non-autorisé ou un accès abusif[1263].

1547 Il sied encore de relever qu'avec la modification de l'art. 56 al. 1 nLPol/GE, le législateur genevois a voulu autoriser la vidéosurveillance employée à titre préventif par l'autorité policière en respectant les critiques formulées par le Tribunal fédéral à l'encontre des anciennes dispositions de la LPol/GE[1264].

c) La vidéosurveillance invasive du domaine privé ou secret

1548 La vidéosurveillance invasive est utilisée par le ministère public aux fins de la recherche de la vérité, notamment à l'aide de la collecte et de l'enregistrement des données pouvant servir de preuve. En tant que dispositif technique de surveillance – comprenant notamment les appareils évoqués aux art. 179*bis* et 179*quater* CP[1265] –, les systèmes de surveillance caméra font partie des "autres mesures techniques de surveillance" prévus aux art. 280 ss CPP. Cette disposition permet de mettre en œuvre une surveillance caméra et non pas d'utiliser des bandes-vidéo déjà capturées. Lorsque la police récupère des images filmées par une installation de vidéosurveillance préexistante afin de déterminer le déroulement des faits, il s'agit d'un séquestre (art. 246 CPP)[1266].

1549 L'autorité pénale est donc autorisée – sous certaines conditions – à utiliser la vidéosurveillance pour observer et/ou enregistrer des conversations ou actions se déroulant dans des lieux non-publics ou qui ne sont pas librement accessibles au public (art. 280 let. b CPP)[1267].

1550 La compétence pour ordonner oralement ou par écrit la mise en œuvre de la surveillance par caméra revient au ministère public. Si l'ordre est donné oralement, une confirmation écrite

---

[1263] Projet de loi du Conseil d'Etat de Genève sur la protection des données personnelles (LPDP) – PL 9870, p. 62-63; Supra Partie II, Chapitre 3, I, B, 2, c, i, c), n° 1508 ss.

[1264] ATF 140 I 381; Projet de loi modifiant la loi sur la police (LPol) - PL 11664.

[1265] MOREILLON, PAREIN-REYMOND, art. 280 N 3; SCHMID, Praxiskommentar, art. 280 N 2; StPO-HANSJAKOB, art. 280 N 2.

[1266] Au sujet de la notion de séquestre, voir: Infra Partie II, Chapitre 3, III, A, 3, c, iii, n° 2058 ss.

[1267] BSK-StPO-KATZENSTEIN, EUGSTER, art. 280 N 28 ss; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 270; PIQUEREZ, MACALUSO, p. 520; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 465; RÉMY, p. 112; RIKLIN, Strafprozessordnung, art. 280 N 3; SCHMID, Praxiskommentar, art. 280 N 9.

afin de documenter les actes de procédure doit exister (art. 76 ss CPP)[1268]. S'il est nécessaire d'entrer dans une habitation ou tout type de domicile (art. 186 CP) pour installer une caméra de surveillance, l'autorisation du ministère public doit être couplée avec un mandat de perquisition (art. 241 al. 1 et 245 al. 1 CPP)[1269].

1551 Dans les grandes lignes, la procédure – demande d'autorisation et informations utilisables – pour exercer la surveillance à l'aide d'appareils de prise de vue est identique à celle régissant la surveillance des télécommunications (art. 269 à 279 CPP *via* art. 281 al. 4 CPP)[1270]. Nonobstant l'applicabilité des art. 269 à 279 CPP, quelques points spécifiques à l'utilisation des autres moyens de surveillance méritent notre attention.

1552 L'art. 281 al. 1 et 2 CPP prévoit que la surveillance ne peut être ordonnée que contre un prévenu. Les tiers, au sens de l'art. 270 let. b CPP, ne sont donc pas concernés par cette surveillance sous réserve de leurs locaux ou de leurs véhicules qui peuvent faire l'objet d'une surveillance si le prévenu s'y trouve ou les utilise[1271]. La possibilité de surveiller les locaux ou véhicules appartenant à un tiers connaît toutefois une exception. Lorsque le tiers entre dans une des catégories visées aux art. 170-173 CPP, la surveillance est interdite (art. 282 al. 3 let. b CPP) sauf si le secret professionnel n'est manifestement pas menacé[1272].

1553 L'interdiction de surveiller s'étend en outre au prévenu en détention lorsqu'il s'agit d'obtenir des preuves (art. 282 al. 3 let. a CPP). Cette interdiction découle directement du noyau intangible de la protection de la liberté personnelle (art. 10 al. 2 Cst) et du droit à la sphère privée (art. 13 al. 1 Cst).

1554 En outre, la vidéosurveillance et tout dispositif technique de surveillance entrant dans la catégorie visée par les art. 280-281 CPP causent une atteinte plus intrusive aux droits de la personnalité et à la sphère privée de l'individu concerné que la surveillance des

---

[1268] CR-CPP-CHIRAZI, art. 241 N 14; SCHMID, Praxiskommentar, art. 280 N 4.

[1269] MOREILLON, PAREIN-REYMOND, art. 280 N 12; RIKLIN, Strafprozessordnung, art. 280 N 4; SCHMID, Praxiskommentar, art. 280 N 4.

[1270] Supra Partie II, Chapitre 3, I, A, 2, c, iv, n° 1171 ss.

[1271] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 237; GOLDSCHMID, Überwachungsmassnahmen, p. 166-167; MOREILLON, PAREIN-REYMOND, art. 281 N 3; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 467; SCHMID, Praxiskommentar, art. 281 N 2.

[1272] CPP-Commentario-MELI, art. 281 N 3; CR-CPP-BACHER, ZUFFEREY, art. 281 N 4; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 216; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 271; MOREILLON, PAREIN-REYMOND, art. 281 N 10; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 467-468; SCHMID, Praxiskommentar, art. 281 N 7.

télécommunications (art. 269 al. 1 let. a CPP). C'est pourquoi l'exigence quant aux soupçons de commission d'une infraction est plus élevée[1273].

d) La vidéosurveillance invasive des espaces publics

1555 La vidéosurveillance invasive des espaces publiques se distingue de la vidéosurveillance préventive par le fait qu'elle est secrète et intervient après la commission d'une infraction[1274] excluant l'applicabilité de la législation sur la police. Elle se distingue également des autres mesures techniques de surveillance par le fait qu'elle n'observe pas des actions dans des lieux privés ou non librement accessibles au public.

1556 La vidéosurveillance invasive des espaces publics au sens large s'effectue dans le dessein de poursuivre les auteurs d'une infraction. Elle est dirigée contre une ou des personnes spécifiques et se planifie sur une certaine durée[1275]. Par conséquent, il s'agit d'une observation – qui se définit comme "[la] *surveillance systématique d'événements et de personnes sur la voie publique pendant un certain temps dans le cadre de la poursuite pénale*"[1276] – au sens des art. 282 et 283[1277].

1. Les conditions d'application

1557 L'art. 282 CPP prévoit que le ministère public et, pendant l'investigation policière, la police peuvent observer secrètement des événements ou des personnes sises dans un lieu librement accessible au public et effectuer des enregistrements.

1558 La mise en œuvre de la vidéosurveillance invasive est admissible moyennant l'existence d'indices concrets laissant présumer que des crimes ou des délits ont été commis (art. 282 al. 1 let. a CPP) et que d'autres formes d'investigations n'auraient eu aucune chance ou seraient excessivement difficiles (art. 282 al. 1 let. b CPP). Les principes de la proportionnalité et de la subsidiarité sont donc expressément consacrés par la base légale.

[1273] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 271.

[1274] Message, CPP, p. 1235.

[1275] BSK-StPO-KATZENSTEIN, EUGSTER, art. 282 N 1-9; CR-CPP-GUÉNIAT, HAINARD, art. 282 N 3; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-BÄTTIG, p. 272; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 472-473; RIKLIN, Strafprozessordnung, art. 282 N 4; SCHMID, Praxiskommentar, art. 282 N 4.

[1276] Message, CPP, p. 1235.

[1277] DONATSCH, SCHWARZENEGGER, WOHLERS, p. 238; DUBUIS, p. 211; PIQUEREZ, MACALUSO, p. 520-521; RIEDO, FIOLKA, NIGGLI, p. 333-334; RUCKSTUHL, DITTMANN, ARNOLD, p. 271.

1559 Aux fins du respect du premier principe, la notion d'indices concrets doit s'interpréter à la lumière du cadre fixé pour l'admissibilité des mesures de contrainte (art. 197 al. 1 CPP). Contrairement aux mesures de surveillance et autres dispositifs techniques (art. 269 ss et 280 ss CPP) jugés plus graves au niveau des atteintes aux droits fondamentaux, l'observation n'est pas restreinte à un catalogue d'infractions et peut servir à observer l'auteur d'un délit de peu de gravité ou d'actes préparatoires[1278]. L'intensité des soupçons étant directement liée à la gravité de l'atteinte causée, en cas d'observation, la force du soupçon peut être nettement plus faible que celle demandée pour la vidéosurveillance invasive sur domaine privé.

1560 Le second principe offre un large pouvoir d'appréciation à la police qui est la mieux placée pour déterminer, dans chaque cas d'espèce, si oui ou non l'observation par vidéosurveillance est plus simple et plus rapide pour atteindre le but recherché.

1561 Sous l'angle de la procédure pénale, il est important de relever que la loi requiert une autorisation (art. 272 al. 1 CPP *cum* 281 al. 4 CPP) si l'action se déroule dans un endroit qui n'est pas public ou pas librement accessible. En revanche, même si l'action est de nature privée, si elle est observée dans un lieu ouvert au public alors l'autorisation du tribunal des mesures de contrainte n'est pas requise. Cette différence entre les divers moyens de surveillance s'explique par le fait que l'observation ne constitue pas une atteinte importante aux droits fondamentaux dès lors que les actions observées et enregistrées se déroulent sur domaine public[1279].

1562 Cependant, afin d'éviter les abus et pour protéger au mieux les droits de la personnalité des individus concernés, l'observation réalisée par la police avant l'ouverture d'une procédure par le ministère public doit être autorisée par celui-ci lorsqu'elle dépasse un mois dès le début effectif de la surveillance (art. 282 al. 2 CPP)[1280].

2. La communication à la personne observée

1563 Dans le respect des droits de la défense – droit de recourir en vertu des art. 393-397 CPP – et sauf exception – non-usage ou intérêt prépondérant –, l'individu filmé est informé de

[1278] CR-CPP-GUÉNIAT, HAINARD, art. 282 N 6; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 474-475; RIEDO, FIOLKA, NIGGLI, p. 335; SCHMID, Praxiskommentar, art. 282 N 10.

[1279] BSK-StPO-KATZENSTEIN, EUGSTER, art. 282 N 9 ss; CR-CPP-GUÉNIAT, HAINARD, art. 282 N 11; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-BÄTTIG, p. 272; SCHMID, Praxiskommentar, art. 280 N 2-3.

[1280] Message, CPP, p. 1236; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 483; SCHMID, Praxiskommentar, art. 282 N 16.

l'existence, du motif et de la durée de la vidéosurveillance effectuée à son encontre au plus tard lors de la clôture de la procédure préliminaire (art. 283 CPP).

1564 Les proches du prévenu dont l'observation a induit l'élucidation des faits doivent également être informés de la surveillance. La notion de proche s'entend au sens large et inclut par conséquent les relations amicales[1281].

1565 En cas de recours, le prévenu et son représentant ne sont pas disposés à obtenir le dossier complet d'observation comprenant les retranscriptions écrites de tous les événements relevés. Seuls les actes d'ordre de mission, les ordonnances et les rapports contenant des informations déterminantes à l'enquête et/ou probantes leur sont fournis.

3. L'exploitation des informations obtenues, des découvertes fortuites et des preuves obtenues illégalement

1566 Les art. 282 et 283 CPP sont muets sur la documentation à verser au dossier, l'exploitabilité des découvertes fortuites ou encore l'inexploitabilité de certaines informations.

1567 La police a un devoir général de documentation. Vraisemblablement, en cas de vidéosurveillance sur domaine public, elle doit constituer un journal d'observation incluant la retranscription des événements et les enregistrements visuels. Les éléments utiles à la procédure doivent en outre être intégrés dans un rapport officiel pour être accessibles aux parties.

1568 En cas de découvertes fortuites, le silence de la loi mène à penser que la découverte de la commission d'un crime ou d'un délit peut être dénoncée et que les preuves obtenues sont exploitables. La doctrine précise qu'hormis la restriction du crime ou du délit, les autres conditions de l'art. 282 al. 1 CPP n'ont pas besoin d'être considérées[1282]. En outre, la manière de procéder en cas de découvertes fortuites relève de l'art. 243 CPP impliquant la mise en sûreté des informations et la transmission immédiate à la direction de la procédure d'un rapport[1283]. Elles sont alors exploitables après détermination de la direction de la procédure et si les conditions légales posées à leur obtention sont réalisées[1284].

[1281] Message, CPP, p. 1236.

[1282] Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 481-482; SCHMID, Praxiskommentar, art. 282 N 11 et 19; StPO-HANSJAKOB, art. 282 N 34.

[1283] SCHMID, Praxiskommentar, art. 282 N 11.

[1284] HAUSER, SCHWERI, HARTMANN, p. 352; SCHMID, RPS, p. 305.

1569 Concernant les preuves obtenues illégalement, par exemple en cas d'observation dans un lieu non-accessible au public ou d'observation de plus d'un mois par la police sans autorisation du ministère public, elles ne sont pas admissibles au procès faute de respecter la règle de validité sur l'exploitation des preuves (art. 141 al. 1 CPP).

4. La fin de l'observation

1570 Lorsque l'ordre d'observation provient du ministère public, même si elle a débuté durant la phase d'investigation policière, il est le seul compétent pour y mettre fin.

1571 Dans les cas où le délai d'un mois n'est pas échu et que l'observation a été ordonnée par la police, c'est cet organe étatique qui peut déclarer la fin de la mesure.

1572 Qu'il s'agisse d'une décision du ministère public ou de la police, l'ordre de mettre fin à l'observation est soumis à la forme écrite sans qu'aucune motivation ne soit obligatoirement énoncée[1285].

3. L'usage et le moyen probatoire

1573 L'évolution importante de la criminalité tant du point de vue de la fréquence que de la nature des infractions commises a nécessité une réaction de la part de l'autorité pénale pour sécuriser et rassurer la population.

1574 Considérée comme un moyen de prévention efficace et qui permet d'établir le déroulement d'un acte délictuel[1286], voire d'identifier le coupable, la vidéosurveillance s'est vite imposée comme un moyen adéquat pour répondre à l'insécurité et permettre de gérer la délinquance, voire poursuivre les auteurs d'infractions[1287].

[1285] CR-CPP-GUÉNIAT, HAINARD, art. 283 N 12.

[1286] Infra Partie II, Chapitre 3, I, B, 4, n° 1592 ss.

[1287] BAUER, FREYNET, p. 4-5; KLAUSER, CCTV, p. 145-146; VILLE DE GENÈVE, vidéosurveillance, p. 2.

a. L'efficacité de la vidéosurveillance dissuasive

1575 Dans le cadre de notre sujet, la vidéosurveillance dissuasive dans son but premier de dissuader ou prévenir les infractions et de lutter contre l'insécurité est de second plan. Nous nous attardons donc uniquement sur la question de son efficacité.

1576 Selon une étude de Baptiste Viredaz[1288], la présence des caméras sur le domaine privé ou public diminue la criminalité de 20 à 30%, ce que contredisent partiellement certaines études effectuées sur territoire anglais[1289].

1577 En tout état de cause, les études sur le sujet doivent être nuancées. En effet, l'efficacité de la vidéosurveillance dissuasive dépend étroitement des formes de délinquance et de criminalité[1290]. Il est évident que la vidéosurveillance exercée par l'autorité n'est pas efficace contre les violences domestiques à l'intérieur d'un logement, par exemple. Ainsi, selon les circonstances et les lieux[1291], l'efficience du système de surveillance par caméra est extrêmement variable.

1578 En contrariété avec les études démontrant une baisse de criminalité, certains réfractaires à la vidéosurveillance plaident en faveur d'un déplacement de la criminalité dans des lieux non-surveillés. Si cela est en partie vrai, l'augmentation de la criminalité dans les lieux sans caméra est moins importante que la diminution de la commission d'actes délictuels dans les espaces surveillés et les zones avoisinantes. Nous constatons en effet que la prévention découlant de la présence de caméra en un lieu rayonne dans les lieux alentours[1292].

1579 Nonobstant les avis réfractaires concernant l'efficacité préventive, l'opinion publique s'accorde à reconnaître que la vidéosurveillance rassure et aide à la tranquillité publique. Il s'agit dès lors plus d'un sentiment psychologique de sûreté que d'une réelle efficience. Certes, la vidéosurveillance a un pouvoir dissuasif, aide la police à déterminer les lieux à risque où potentiellement une patrouille devrait être envoyée, mais elle n'est pas une barrière absolue contre les crimes ou les délits. Ainsi, ce moyen de surveillance doit s'additionner avec d'autres tâches sécuritaires.

[1288] INHES, p. 11-13; VIREDAZ, insécurité, p. 76 ss.

[1289] A ce sujet, voir: WELSH, FARRINGTON, p. 41-42.

[1290] BAUER, FREYNET, p. 30; CUSSON, RICPTS, p. 141-142.

[1291] KLAUSER, CCTV, p. 155-156; KLAUSER, Videoüberwachung, p. 107-114.

[1292] CORNU, p. 253; KLAUSER, Videoüberwachung, p. 107-114.

b. Les informations recueillies par vidéosurveillance et leur valeur probatoire

1580 En tant que données ou informations visuelles, la vidéosurveillance est utile à la procédure pénale.

1581 Quel que soit le type de vidéosurveillance, qu'elle soit dissuasive ou invasive, les images capturées peuvent servir pour détecter un événement et obtenir des informations. Certes, la finalité première de la vidéosurveillance dissuasive n'est pas d'obtenir des informations sur la commission d'une infraction. Néanmoins, il n'est pas exclu que son but dissuasif ne soit pas réalisé, qu'un acte délictuel ait lieu et qu'ainsi les images puissent être utiles à l'enquête policière et à la justice[1293].

1582 Corrélativement à la preuve issue de la surveillance des télécommunications, la vidéosurveillance avec enregistrement simple ou informatisé fournit un certain nombre d'informations sous forme d'images qui sont parfois utiles à la procédure et parfois non. Pour administrer les images au cours d'une procédure pénale, il est donc important d'effectuer un tri afin, notamment, de limiter au maximum l'atteinte aux droits fondamentaux.

1583 En tant que preuve dite matérielle, la valeur probatoire des captures effectuées à l'aide d'une caméra dépend étroitement de leur authenticité et de leur véracité. C'est pourquoi, même si un tri des données utiles ou inutiles est nécessaire, en toute hypothèse, la totalité des images filmées et enregistrées doivent être conservées sous leur forme originale afin de pouvoir prétendre à une valeur probatoire élevée.

1584 Quant aux images filmées par les personnes privées, ce qui prévaut à l'enseigne de l'interception et de l'enregistrement des communications et de l'administration d'une preuve illicite par les particuliers est applicable à la vidéosurveillance[1294].

1585 En conséquence, pour autant que la vidéosurveillance effectuée respecte la procédure ou si tel n'est pas le cas – mais que l'autorité aurait pu se procurer les images d'une manière conforme au droit – que la pesée des intérêts plaide en faveur de leur exploitabilité[1295], les images issues de cette surveillance sont admissibles comme moyen probatoire au procès

---

[1293] CORNU, p. 254; RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 84.

[1294] Supra Partie I, Chapitre 3, B, 3, e, n° 311 et 332 et 337; Supra Partie II, Chapitre 3, I, A, 2, d, n° 1226 ss.

[1295] ATF 109 Ia 244, 246-248 = JdT 1984 IV 160 = SJ 1984 153, 155-157; ATF 131 I 272, 278-282; ATF 137 I 218, 223-224 = JdT 2011 I 354, 358-359; ATF 138 IV 169, 171; TF 1B_22/2012 du 11 mai 2012, c. 2.4.4; CourEDH, Affaire *Teixeira de Castro c. Portugal*, arrêt du 9 juin 1998, 25829/94, § 34; CourEDH, Affaire *Schenk c. Suisse*, arrêt du 12 juillet 1988, 10862/84, § 46; CourEDH, Affaire *Allan c. Royaume Uni*, arrêt du 5 novembre 2002, 48539/99, § 42; CourEDH, Affaire *Gafgen c. Allemagne*, arrêt du 1er juin 2010, 22978/05, § 162-168.

pénal pour identifier les auteurs d'infractions ou pour déterminer les circonstances de certains crimes ou délits[1296].

4. La discussion sur la preuve obtenue par vidéosurveillance

1586 Comme pour toutes les preuves, la technicité et les possibilités de visualiser et/ou de traiter les bandes-vidéo enregistrées ne fournissent pas l'absolue vérité. Il faut, par conséquent, peser le pour et le contre en analysant les forces et les faiblesses de la vidéosurveillance en tant qu'elle fournit des données utilisables comme preuve pénale.

a. Le potentiel de la vidéosurveillance

i. La nature de la preuve obtenue par vidéosurveillance ou technique audio-visuelle

1587 La vidéosurveillance transporte virtuellement le juge et l'autorité policière sur les lieux de commission d'une infraction. Par conséquent, elle se révèle être un moyen approprié de reconstitution et d'étude d'événements qui permet dans certaines circonstances de confirmer adéquatement les soupçons de l'autorité policière et/ou judiciaire.

1588 L'exploitation de la vidéosurveillance devant les tribunaux pénaux est assimilable à la présentation matérielle des faits. Contrairement aux témoignages reflétant les souvenirs et l'interprétation du témoin[1297], les images capturées par des caméras et fixées sur un support sont dénuées de subjectivité. C'est pourquoi un crédit important est accordé à ce moyen de preuve jugé comme étant représentatif de la réalité.

1589 Nous pourrions considérer que le tri des informations et leur interprétation nuisent à l'objectivité des images visualisées. Il faut néanmoins tempérer cette inquiétude et différencier les images qui sont objectives et la démonstration issue de cette preuve entachée de subjectivité.

1590 Concernant le tri des informations, la totalité des données ne sont pas visionnées au tribunal. Seules les séquences jugées utiles pour établir les faits et/ou pour identifier l'accusé sont présentées à la Cour. Comme tout choix, même si celui-ci est cadré par la règle de la nécessité, il n'en demeure pas moins qu'une part de subjectivité existe. Pour contrer les

[1296] BÜLLESFELD, p. 23; MÉTILLE, Thèse, p. 84-85; VILLE DE GENÈVE, vidéosurveillance, p. 3.

[1297] Supra Partie I, Chapitre 3, IV, A, 2, n° 332 ss.

inquiétudes quant au séquençage des enregistrements, la conservation de la totalité des images permet au juge, en cas de besoin, de visionner plus d'éléments et de se faire une idée réelle des événements.

1591 Quant à l'interprétation réalisée suite au visionnage des images par la Cour, l'accusation ou la défense, elle implique immanquablement un élément de subjectivité. Néanmoins, cette subjectivité intervient en aval de la capture et de l'enregistrement des images. Elle n'influence donc pas la qualité objective de la vidéosurveillance en tant que technique probatoire. En revanche, la preuve administrée est une preuve scientifique qui, comme toute preuve, doit être libre et permettre au juge d'obtenir ou non l'intime conviction. Par conséquent, la subjectivité n'est pas liée au dispositif technique ou aux données enregistrées, mais bien à son intégration par les juristes lorsqu'il s'agit de déterminer l'établissement des faits à l'aide des images visionnées.

1592 Par conséquent, les images capturées et traitées restent – normalement[1298] – une représentation fidèle de la réalité et donc fournissent un moyen de preuve avec une force de conviction importante.

ii. La vidéosurveillance comme un moyen de preuve à charge ou à décharge

1593 Nous l'avons vu[1299], la vidéosurveillance est utile tant pour identifier les auteurs d'infraction que pour établir les circonstances de commission d'un crime ou d'un délit. De manière similaire aux autres preuves analysées, la vidéosurveillance est une preuve à charge et à décharge[1300]. Nous ne développons dans la présente partie que ce qui relève spécifiquement de la vidéosurveillance.

1594 Au-delà d'innocenter un prévenu ou une tierce personne parce qu'il ne se trouvait pas sur les images filmées, qu'il ne s'agissait en réalité pas de lui ou d'elle ou que les images démontrent un déroulement différent des faits, la vidéosurveillance permet de démontrer qu'un témoin n'a en réalité rien vu parce qu'il faisait dos à la scène. Ainsi, ce dispositif technique permet de mettre en doute la valeur de certaines autres preuves ou mettre l'accent sur les faiblesses des témoignages et, en finalité, de placer le juge décideur dans un rôle similaire à celui du

[1298] Infra Partie II, Chapitre 3, I, B, 4, a, ii, n° 1592 ss; Infra Partie II, Chapitre 3, I, B, 4, b, i, n° 1616 ss.

[1299] Supra Partie II, Chapitre 2, I, B, 3, b, n° 1580 ss.

[1300] CORNU, p. 255. Supra Partie II, Chapitre 2, I, C, 1, a, iii, n° 650 ss; Supra Partie II, Chapitre 2, II, C, 1, a, i, n° 946; Supra Partie II, Chapitre 3, I, A, 4, a, ii, n° 1259 ss.

témoin. En effet, grâce aux images, il peut voir, comme le verrait un témoin, les circonstances et le déroulement des actes à juger.

1595 En outre, grâce au techniques audiovisuelles, les magistrats ont la possibilité d'avoir une vue directe sur les interrogatoires ou les auditions des témoins et du ou des suspects. Ainsi, ils peuvent apprécier directement le degré de spontanéité des déclarations, l'état d'esprit de la personne interrogée et son attitude générale. Il n'est alors plus question de s'appuyer sur le procès-verbal ou sur des déclarations tierces, ce qui renforce considérablement la position du juge face aux preuves administrées.

1596 Parallèlement au renforcement de la position de l'autorité pénale en ce qui concerne l'établissement des faits, la défense n'a plus les mêmes facilités – par exemple – pour réfuter les faits ou arguer l'utilisation de la contrainte, de la violence, etc. pouvant mettre à mal un interrogatoire et entacher les aveux d'un suspect[1301]. D'un autre point de vue, des images peu claires, imprécises ou au contraire démontrant clairement que l'accusé n'est pas le responsable de la commission d'un crime ou d'un délit rendent les déclarations de l'accusation fragiles et non tangibles.

1597 Malgré sa supposée force de démonstration, afin d'éviter que le fardeau de la preuve ne soit renversé et que l'individu concerné doive alors prouver la fausseté ou l'inexactitude des images, il est impératif que la vidéosurveillance ou les techniques audiovisuelles ne soient pas considérées comme une solution irréprochable, concrète et réelle sans pouvoir être entachées de faussetés, d'incohérences ou d'inexactitudes. Ainsi, les autorités pénales ne peuvent pas s'appuyer sur cette unique preuve sans plus d'investigation.

1598 En conséquence, avec une bonne organisation, des systèmes adéquats et une procédure de mise en œuvre et d'exploitation respectée, les systèmes audiovisuels et de vidéosurveillance fournissent un moyen probatoire avec une force de conviction pouvant être reconnue par certaines personnes comme comparable à l'aveu dans le système inquisitoire. Cependant, malgré le regard direct que la justice peut porter au déroulement des faits de l'affaire à juger, ce mode probatoire n'est pas absolu et ne peut pas constituer l'unique preuve[1302].

[1301] MCDONALD, p. 78-79.

[1302] Infra Partie II, Chapitre 3, I, B, 4, b, n° 1618, 1628, 1632 et 1638.

iii. Les procédés techniques limitant la portée et la capture réalisées par les caméras

1599 Du point de vue de la protection des données, il n'y a aucune objection à l'utilisation de la vidéosurveillance pour diminuer le sentiment d'insécurité ou obtenir un moyen probatoire tant qu'aucune atteinte inadmissible aux droits et libertés liées au traitement des données n'existe. Cependant, il est indispensable que les données récoltées soit propres et nécessaires à atteindre le but visé par la mise en place du système de surveillance caméra sans quoi le principe de proportionnalité ne peut pas être reconnu.

1600 Avec le zoom qui accentue le champ de vision des caméras et la haute résolution, des craintes d'être filmé sans le savoir et de porter atteinte aux droits fondamentaux d'un grand nombre d'individus sans que cela ne soit justifié sont nées.

1601 Les critères que nous allons développer n'influencent pas en soi la valeur probatoire de la vidéosurveillance. Néanmoins, une preuve violant les droits fondamentaux ou la loi de manière inadmissible n'est pas exploitable. Un système technique trop envahissant, réduisant les libertés à leur strict minimum, sans intérêt public ou sans pesée des intérêts va à l'encontre de la confiance que tout citoyen a envers la justice, s'il est utilisé comme preuve.

1602 Grâce aux nouvelles technologies, de nombreux procédés existent pour éviter les atteintes trop importantes aux libertés personnelles. Ainsi, le détecteur de mouvement, le floutage des images et la réduction du champ de vision des caméras permet aux autorités de réaliser leurs tâches – dissuader ou réprimer les auteurs d'infraction – sans que des tiers innocents n'ayant causé un acte délictuel soient filmés fréquemment dans divers lieux et à divers moments, notamment sur la voie publique.

a) La détection de mouvements

1603 La détection des mouvements offre la possibilité de détecter les comportements anormaux.

1604 Grâce à des algorithmes de comportements "acceptables" ou "normaux", il est possible de repérer ceux jugés "déviants"[1303].

1605 Cette technologie seule est utile pour aider à la détection des infractions.

[1303] LAPORTE, p. 30.

1606 Couplée avec un système de floutage, il est possible de diminuer considérablement la gravité de l'atteinte aux libertés personnelles et à la sphère privée[1304].

b) La vidéosurveillance intelligente

1607 La vidéosurveillance intelligente permet de brouiller les personnes et les objets mobiles afin d'assurer l'anonymat, étant précisé que l'opération de brouillage est réversible[1305].

1608 Ainsi, il est possible de surveiller des lieux publics ou accessibles au public sans porter atteinte à la sphère privée puisque les données cryptées ne permettent pas d'identifier la ou les personnes filmées.

1609 Lorsqu'un comportement jugé suspect est détecté, l'autorité compétente visionne l'enregistrement et, s'il apparaît qu'une infraction a été commise, les images sont décryptées. Ainsi, cette technologie évite que tout un chacun soit filmé de manière à être immédiatement identifié ou identifiable.

1610 Relevons encore que le floutage des images peut également être partiel ce qui permet de garder l'anonymat sur d'éventuels co-enregistrés qui ne seraient pas mis en cause dans la commission de l'acte délictuel.

1611 Nonobstant la qualité de cryptage et la diminution des atteintes aux droits fondamentaux, la vidéosurveillance intelligente ne garantit pas que les données ne soient pas utilisées abusivement. C'est pourquoi la solution la plus adéquate est de limiter le décryptage et l'accès aux données décryptées à un cercle restreint de personnes, voire d'utiliser une double clé de cryptage ou de créer un journal des accès[1306].

c) La réduction du champ de vision

1612 La réduction du champ de vision des caméras a la propriété d'éviter que des lieux privés ou relevant du domaine secret soient filmés.

1613 Prenons l'exemple d'une caméra de surveillance positionnée à but dissuasif sur un immeuble. Le champ de vision englobe la vue dans son ensemble et la fenêtre d'un

[1304] ATF 138 II 346, 366-372 = JdT 2013 I 71, 91-94.

[1305] Supra Partie II, Chapitre 3, I, B, 1, c, n° 1443 et 1446.

[1306] PFPDT, Rapport 2007/2008, p. 28; PFPDT, Rapport 2008/2009, p. 22.

appartement se trouvant sur la façade dudit immeuble. Deux solutions existent pour éviter que les images capturées relèvent du domaine secret ou privé (art. 179*quater* CP): réduire le champ de vision par des systèmes de blocage ou compléter le système de vidéosurveillance avec un logiciel de floutage.

1614 Grâce aux procédés techniques de limitation du champ de vision ou de la visualisation des images, il est possible de délimiter convenablement les zones filmées. Ainsi, il devient plus aisé de veiller à ce que l'atteinte aux libertés ne soit pas disproportionnée tout en permettant une surveillance adéquate[1307].

d) La destruction automatique des informations captées et enregistrées

1615 La destruction automatisée des images joue également un rôle dans le cadre du respect et de la garantie de la protection des droits fondamentaux[1308].

1616 Toutes les images ne peuvent pas être conservées, stockées et traitées après un certain délai. Sous le couvert du respect de la proportionnalité, les informations qui ne sont pas utiles comme moyen de preuve doivent être effacées rapidement.

b. Les problématiques liées à la preuve issue de la vidéosurveillance

i. La qualité des images et leur modélisation bidimensionnelle

a) La manipulation des images

1617 La manipulation des images et du son nuit à l'objectivité de la vidéosurveillance.

1618 Actuellement, il existe un certain nombre de logiciels permettant de retravailler les images impliquant un risque quant à la garantie de l'authenticité des faits capturés et des personnes filmées, principalement quand la vidéosurveillance a été exécutée par un particulier[1309].

1619 Le risque de manipulations rend parfois la preuve par la vidéosurveillance fragile. C'est pourquoi des investigations doivent être réalisées pour s'assurer de la véracité et de

[1307] RUEGG, FLÜCKIGER, NOVEMBER, KLAUSER, p. 85.

[1308] TF 1C_363/2014 du 13 novembre 2014, c. 2 = SJ 2015 I 128, 129-130; ATF 133 I 77, 83-88 = JdT 2008 I 418, 424-429; ATF 136 I 87, 116-117 = JdT 2010 I 367, 393-394.

[1309] FICHET-BOYLE, p. 214; LEGLER, p. 202.

l'inexistence de manipulations visuelles sur les enregistrements fournis comme moyen de preuve.

1620 En outre, il est essentiel qu'une personne qualifiée certifie que le système de surveillance caméra n'a pas subi de défaillance technique, que les images sont authentiques ou, si elles sont retravaillées, l'implication que cela peut avoir sur la validité de la preuve. Malgré cette protection, le juge ne peut jamais être totalement certain de l'authenticité des images, ce d'autant que, bien souvent, les données manipulées sont difficilement décelables car elles gardent des apparences d'exactitude.

b) Le traitement des images

1621 La démocratisation des techniques s'est accompagnée de l'accès des particuliers à la vidéosurveillance et aux caméras en tout genre. Selon le type de caméras employées – spécifiquement faites pour la surveillance, caméras numériques, de téléphones portables –, la qualité de l'image varie.

1622 Les données enregistrées, principalement par les particuliers, de mauvaise qualité doivent subir divers traitements – défloutage, super-résolution – pour livrer tout leur potentiel et écarter les images non nécessaires à l'enquête et à la procédure pénale. Ainsi, les images dites amateurs ou dont la qualité visuelle est moindre n'ont forcément pas la même force probatoire qu'une image nette, réalisée dans des conditions de luminosité adéquates et avec une caméra de haute technologie.

1623 Par ailleurs, il n'est pas exclu que, pour des raisons techniques, l'image floue, imprécise ou extrêmement pixélisée soit inutilisable, même après traitement. En effet, les meilleurs systèmes de traitement d'images ne peuvent pas recréer des pixels manquants ou rendre absolument nette une image floue[1310]. Parfois, le traitement est également impossible rendant la vidéosurveillance inutile, par exemple, parce que des branches ou feuilles d'arbre obstruent le champ de vision, que la pluie tombe sur l'objectif brouillant l'image, etc.[1311]

1624 Martin Gill et Angela Springs ont relevé dans leur étude que les images filmées de nuit d'environ 50% des caméras analysées étaient inutilisables ou quasiment par manque de luminosité ou, au contraire, par éblouissement d'une lumière sise trop prêt de l'objectif[1312].

[1310] BAUER, FREYNET, p. 48.

[1311] ASSOCIATION SOURIEZ-VOUS ETES FILME, p. 9.

[1312] GILLS, SPRIGGS, p. 78.

Les données capturées doivent alors obligatoirement être traitées pour être exploitables comme preuve, perdant ainsi leur authenticité et ne reflétant possiblement plus la réalité.

1625 Les progrès technologique ne font pas de miracle: ce qui n'existe pas ne peut pas être reconstitué, tout du moins sans que cela touche à l'authenticité et à la véracité des données.

c) La visualisation en deux dimensions d'une réalité en trois dimensions

1. La problématique de la vision en deux dimensions

1626 La perception visuelle issue de la vidéosurveillance est également un point à ne pas négliger. Il est impératif de garder à l'esprit que les images capturées visant à identifier les auteurs et le déroulement des infractions sont une vision bidimensionnelle de faits réels tridimensionnels.

1627 Corrélativement à la problématique énoncée pour les empreintes digitales[1313], la modélisation en 2D d'un événement en 3D ou d'un visage en 3D implique une perte d'informations plus ou moins importante.

1628 Prenons l'exemple d'une image fixe, l'objectif visionne le dos d'une personne (A) grâce à un effet d'angle, nous constatons qu'il tend le bras vraisemblablement en direction d'un tiers (B) avec ce qui peut ressembler à une barrette de haschich. Quelques secondes après, A met quelque chose dans sa poche et s'en va. Il est alors arrêté, la fouille permet de trouver sur lui environ 300 CHF. Il est mis en détention pour trafic de stupéfiant, les images visionnées sont apportées comme preuve. En s'appuyant sur les images et le passé de A déjà condamné pour trafic de stupéfiant, le juge décide de le condamner. En réalité, A et B était distants de quelques 5 mètres et ne se sont jamais rencontrés. Néanmoins, l'effet d'optique et de perspective occasionnés par le passage du 3D en 2D montrent que A et B sont physiquement entrés en contact.

1629 Cet exemple démontre que la réalité n'est pas toujours clairement retranscrite par les images de la vidéosurveillance. C'est pourquoi le juge doit analyser correctement ce qu'il visualise, demander un avis à un expert qui pourra l'aider dans la perception de la scène et ne pas apporter trop de crédit à des images ne révélant pas l'exacte vérité.

[1313] Supra Partie II, Chapitre 2, I, C, 1, b, v, n° 720.

2. La modélisation tridimensionnelle

1630 L'évolution technologique peut contrer la problématique de la représentation bidimensionnelle d'un événement tridimensionnel, notamment avec la modélisation 3D qui implique l'existence de plusieurs caméras et d'un logiciel ou encore le simple usage de diverses caméras implémentées individuellement recréant fictivement une vision tridimensionnelle[1314].

1631 Grâce à ces deux mesures, il est possible de modéliser le déroulement d'une scène ou le visage d'un suspect en 3D pour permettre l'identification forensique et formaliser toutes les images[1315]. Couplé avec un logiciel permettant d'extraire des informations spatiales et géométriques du sujet ou de la scène représentée, la modélisation en 3D semble offrir une perception exacte des faits. Ensuite, il s'agit de confronter les images à un état de fait concret pour s'assurer de ce qu'elles démontrent sans omettre le degré d'incertitude dû au traitement tridimensionnel.

1632 Malgré le degré important d'objectivité liée à l'utilisation de la vidéosurveillance comme moyen probatoire, il n'en reste pas moins que la qualité des images et le passage bidimensionnel d'un événement tridimensionnel impliquent des pertes d'informations qui peuvent transformer considérablement la réalité du déroulement de l'acte délictuel ou occasionner un faux-positif dans l'identification d'un suspect.

1633 Il faut donc nuancer l'objectivité de la vidéosurveillance: elle ne représente pas la réalité en tant que telle. Elle n'est qu'une retranscription de la réalité. Conséquemment, des incertitudes subsistent quant à la perfection de la retranscription.

ii. Les pertes d'informations liée à une surveillance incomplète ou aux données retirées

1634 Rodolphe Archipald Reiss a écrit "[…] *l'appareil photographique est l'enregistreur qui voit tout et qui enregistre tout* […]"[1316], nul doute que cette remarque aurait aussi valu pour la caméra et l'enregistreur s'ils avaient existé en 1903. Néanmoins, cet enthousiasme pour les images capturées est erroné.

[1314] A ce sujet, voir: LANZI, CORREVON, SAPIN, DE PRIESTER, p. 233-238.

[1315] CURCHOD, p. 44; MILLIET, p. 45.

[1316] REISS Rodolphe Archibald, *La photographie judiciaire*, Paris 1903, p. 35.

a) La problématique des angles morts

1635 Le champ de vision d'une caméra n'est pas infini. Il n'est dès lors pas exclu qu'un événement débute en un lieu non surveillé ou tout du moins hors champ visuel de la caméra et se déroule ensuite face à la vidéosurveillance. La prise en compte des angles morts des caméras est nécessaire et obligatoire dans le cadre d'une interprétation correcte et complète de la preuve par la vidéosurveillance.

1636 Imaginons l'état de fait suivant: un individu A frappe B en dehors des caméras, commettant une lésion corporelle. Pour éviter un second coup, B frappe A qui subit à son tour une atteinte à l'intégrité corporelle. Ce dernier ayant reculé de quelques pas, ils se trouvent alors tous les deux dans le champ de vision d'une caméra. Le lendemain, A porte plainte contre B, les images de vidéosurveillance sont visionnées. B clame alors la légitime défense, mais le premier coup n'est pas visible sur les enregistrements.

1637 En niant la problématique des angles morts, la légitime défense ne sera vraisemblablement pas reconnue, alors qu'en prenant en compte cette faille, l'investigation policière sera étendue à ce qui s'est passé avant. Ainsi, les chances que le motif justificatif puisse trouver à s'appliquer augmente considérablement changeant ainsi l'issue du procès.

1638 Un mauvais ajustement de la caméra peut également empêcher de constater l'infraction, les circonstances pouvant aider à l'enquête sur un suspect ou encore d'identifier un individu[1317].

1639 Il existe donc des failles qui ne doivent pas être négligées lors de l'analyse, du traitement et de l'interprétation réalisée grâce aux données capturées par les caméras.

b) L'étendue du champ de vision dépendamment de l'utilisation d'une caméra fixe ou mobile

1640 Un deuxième problème relatif au champ de vision vient du système technique de vidéosurveillance ou, plus exactement, du choix opéré entre l'installation d'une caméra fixe ou d'une caméra mobile.

1641 Alors que la caméra fixe a l'avantage de couvrir un champ de vision plus étendu et d'avoir une meilleur qualité d'image, elle ne permet ni de zoomer ni de suivre un suspect qui se déplace. Inversement, la caméra mobile offre ces possibilités.

[1317] LAPORTE, p. 30.

1642 Cependant, un désavantage conséquent existe avec la rotation programmée des caméras mobiles[1318]. En effet, il n'est pas exclu qu'un événement ne soit filmé qu'en partie parce que la caméra bouge et qu'en changeant d'angle, le déroulement des faits de l'acte délictuel ne soit pas capturé et/ou enregistré dans son ensemble.

1643 L'arrêt brusque de la capture par une caméra mobile ou au contraire la prise en cours d'événements délictueux fournit une preuve incomplète, soit imparfaite ce qui diminue considérablement sa valeur pour rechercher la vérité matérielle.

c) Les erreurs d'interprétation des images

1644 Les erreurs d'interprétation peuvent être liées à la saturation du système automatisé ou à l'étape d'analyse des images visionnées dépendante de la subjectivité.

1645 Dans le premier des cas, le système automatisé étant saturé, plus aucune donnée ne peut être conservée. Un certain nombre d'images sont alors manquantes ou ont disparu. Ainsi, les captures ne reflètent pas la réalité ou plus exactement se limitent à une réalité partielle.

1646 Les systèmes de vidéosurveillance ne sont en outre pas à l'abri d'une panne technique de longue ou courte durée, voire de très courte durée presque invisible, qui occasionne l'arrêt de la caméra ou de la transmission réseau. Une panne de plusieurs minutes pose naturellement moins de problème puisqu'elle peut être immédiatement détectée et prise en considération dans l'analyse de la vidéo. Au contraire, une panne de quelques secondes peut passer inaperçue.

1647 Durant le laps de temps où le système ou une partie du système est en panne, les images ne sont plus capturées, enregistrées ou transmises. Néanmoins, le déroulement des faits se poursuit dans la réalité. Il se peut que certains faits soient par ailleurs essentiels à la procédure. C'est pourquoi il est nécessaire de vérifier qu'aucune image n'est manquante – par exemple qu'il n'existe pas de saut d'images d'une seconde ou plus – afin de pouvoir déterminer la qualité de la preuve. Dans l'hypothèse où le magistrat constate la discontinuité des enregistrements, il est indispensable d'en déterminer l'impact pour s'assurer de la valeur probante des données issues de la vidéosurveillance.

1648 Outre les problèmes techniques, l'analyse des images issues de la vidéosurveillance sans enregistrement implique la visualisation en temps réel. Il est illusoire de penser qu'il existe

[1318] ASSOCIATION SOURIEZ-VOUS ETES FILME, p. 9.

un écran par caméra ou encore que les opérateurs puissent surveiller plus d'un écran à la fois de manière correcte. Par conséquent, la plupart des délits échappent tout ou en partie à la vigilance des opérateurs qui, par la suite, ne peuvent pas apporter leur témoignage ou apportent un témoignage ne reflétant pas toute la réalité. Ainsi, seuls les systèmes de vidéosurveillance intégrant la technologie de détection automatique des comportements anormaux peuvent parer à la difficulté de visionnage des opérateurs. Cependant, ceci tend à sous-entendre qu'il est possible de modéliser complètement les comportements relevant d'infractions – identification des comportements suspects et pertinence de suivre le suspect sans pour autant se fonder uniquement sur des stéréotypes ou des préjugés – pour que la détection soit efficace[1319], ce qui, au vu de la nature et de la diversité des infractions, semble difficilement réalisable.

1649 Quant à l'analyse par les criminologues, les experts ou le juge du fond des images enregistrées par un système de vidéosurveillance, elle doit intégrer la totalité des failles présentées ci-dessus. Elle est au surplus relativement subjective. Même si les images présentées montrent des faits réels, nous avons vu qu'il ne s'agissait pas d'une reproduction fidèle de la réalité, que des éléments peuvent être manquants ou refléter une réalité autre. S'ajoute à cela qu'en visualisant les images, le criminologue, l'expert ou le juge intègre ce qu'il a vu dans sa représentation des faits ce qui laisse immanquablement une place à la subjectivité qui peut être erronée.

1650 Concernant les techniques audiovisuelles, les risques liés aux failles techniques sont moindres. Les pannes sont généralement détectées immédiatement et l'interrogatoire ou l'audition peut alors être stoppée. Le seul risque réel reste l'interprétation réalisée suite au visionnage de l'enregistrement.

1651 Par conséquent, qu'importe le système de vidéosurveillance ou audiovisuel, pour garantir un jugement correct, il faut prendre en considération les risques liés à la technicité de la méthode et à l'aspect subjectif de l'interprétation sans quoi une fausse valeur probatoire pourrait être reconnue aux données issues de la vidéosurveillance.

iii. Une valeur ajoutée, mais non pas un moyen d'investigation unique

1652 De façon générale, la vidéosurveillance ne contribue pas notablement à la diminution de la criminalité et ne fournit pas un sentiment de sécurité parfait[1320]. Pour ce dernier point, il est

[1319] LAPORTE, p. 30; LAVENUE, VILLALBA, p. 19.

[1320] CUSSON, RICPTS, p. 136-137; LAPORTE, p. 40.

en effet inimaginable qu'une personne dans la rue puisse se sentir réellement en sécurité grâce à une caméra sachant pertinemment que l'autorité d'intervention est distante du lieu où elle se trouve, sans oublier qu'il n'est pas exclu que des enregistrements vidéo soient réalisés sans surveillance humaine.

1653 En outre, comme nous l'avons énoncé ci-dessus[1321], les images capturées ne correspondent pas forcément à l'entièreté des faits ou ne sont pas analysées correctement, voire elles ne sont pas suffisamment précises ou de bonne qualité pour fournir des éléments pertinents ou de haut intérêt à l'enquête et à la justice.

1654 Pour ces raisons, les systèmes de vidéosurveillance et audiovisuels ne doivent, en aucun cas, se substituer aux autres tâches de police, ni constituer l'unique moyen probatoire à charge ou à décharge administré dans la procédure.

1655 La vidéosurveillance doit se concevoir globalement comme un moyen d'aider la police et la justice[1322].

1656 Par exemple, elle doit servir à enclencher un processus d'alerte afin qu'une équipe d'intervention se déplace sur les lieux où une caméra a filmé un acte délictuel. Dans ce contexte, les systèmes de surveillance sont des outils d'appui censés favoriser la mobilité des agents d'intervention et permettre aux forces policières d'assurer une présence préventive sur un lieu déterminé.

1657 Ainsi, les arrestations – sans lesquelles il n'y aurait pas de jugement et donc pas d'administration de la preuve – peuvent être en nette augmentation si la vidéosurveillance est employée à bon escient.

1658 Quant à la vidéosurveillance invasive, elle ne peut clairement pas être le seul moyen d'enquête lorsqu'un soupçon existe, ce d'autant plus qu'une unique preuve exploitable et administrée au procès ne peut pas être suffisante pour créer le faisceau de preuves essentiel à la recherche de la vérité matérielle.

1659 La vidéosurveillance ne peut remplacer ni un policier, ni une enquête et ne suffit pas par elle-même à prouver le déroulement d'un fait ou à identifier l'auteur d'une infraction, sachant que des soucis techniques peuvent exister, que les images sont parfois peu précises, trop

[1321] Supra Partie II, Chapitre 3, I, B, 4, b, ii, n° 1634 ss.

[1322] BAUER, FREYNET, p. 76-78.

éloignées ou pixélisées, et que les caméras ne filment pas l'entièreté ni du domaine privé ni du domaine public.

1660 Le juge doit pouvoir justifier sa décision à l'aide de preuves fiables démontrant la véracité des circonstances de commission de l'acte délictuel. S'appuyer uniquement sur la vidéosurveillance revient à nier la faiblesse technique des systèmes de surveillance, la qualité des images et la reproduction en deux dimensions d'un fait tridimensionnel.

1661 Par conséquent, la vidéosurveillance dissuasive n'a de sens que si elle est encadrée d'une politique sécuritaire et de moyens humains. Quant à la vidéosurveillance répressive, elle n'a qu'une force probatoire relative. Elle doit donc s'ajouter à d'autres preuves pour créer un faisceau probatoire et permettre la correcte recherche de la vérité.

c. Quelques pistes de réflexion

i. Quelques moyens de précautions à mettre en œuvre

1662 En tant que technique d'investigation portant atteinte au droit constitutionnel, l'utilisation de la vidéosurveillance par les autorités doit respecter les conditions de restriction des droits fondamentaux pour être exploitable en tant que preuve pénale. La condition de la proportionnalité de la mesure est la plus délicate à respecter et celle qui risque le plus facilement de ne pas être remplie.

a) Les méthodes techniques

1663 Afin de limiter les atteintes aux libertés personnelles ou tout du moins que celles-ci ne soient pas disproportionnées, certaines précautions d'ordre technique ou organisationnel peuvent être prises.

1664 Nous l'avons développé précédemment[1323], la mise en œuvre de certaines mesures techniques ou informatiques permet de limiter la gravité de l'atteinte causée aux libertés personnelles:

- le détecteur de mouvement, si tant est que les comportements dits anormaux soient clairement et précisément modélisés, offre l'opportunité de ne filmer que les individus dont le comportement peut faire l'objet d'une poursuite pénale;

[1323] Supra Partie II, Chapitre 3, I, B, 4, a, iii, n° 1599.

- le floutage induit un résultat équivalent puisqu'aucune personne ou objet n'est identifié ou identifiable sans décryptage de l'image qui doit intervenir dans des conditions strictes, notamment suite à un dépôt de plainte ou à la constatation de la commission d'un acte délictuel;
- la réduction du champ de vision tend à limiter l'étendue de la zone filmée, notamment en évitant la capture d'images ressortant du domaine privé ou secret, et ainsi à réduire le nombre d'informations personnelles recueillies.

1665 Toutes ces mesures limitent donc la capture des images amoindrissant la gravité de l'atteinte à la vie privée et à l'autodétermination informationnelle. Ainsi, il est plus aisé de reconnaître la proportionnalité de la mesure de surveillance visuelle.

b) Les conditions de mise en œuvre ou organisationnelles

1666 Un certain nombre de conditions de mise en œuvre de la vidéosurveillance ou d'organisation permettent également une vidéosurveillance proportionnée en encadrant l'enregistrement et le traitement des données capturées:

- la fixation d'un délai maximum de conservation, voire la destruction automatique des images capturées s'il s'avère qu'elles ne sont pas liées à un acte délictuel ou à un dépôt de plainte, répond au principe de proportionnalité;
- lorsque la durée de conservation est relativement longue, une réglementation limitant l'usage abusif des images et le restreignant au but visé permet d'admettre la restriction aux droits fondamentaux[1324];
- la prise de mesures visant à éviter le visionnage par tout un chacun pour des raisons dépassant la finalité de la vidéosurveillance;
- la limitation du droit d'accès aux données stockées;
- la possession de la clé de décryptage par un nombre restreint de personnes soumises au respect de conditions strictes pour décrypter les informations;
- la nécessité d'une double clé pour autoriser le décryptage;
- la communication restreinte à un certain cercle de personnes;
- la sécurisation du lieu de conservation et l'utilisation des seules images strictement nécessaires, etc.

[1324] DFJP, Rapport vidéosurveillance, p. 27.

1667 Toutes ces limitations ainsi que l'instauration d'une procédure d'autorisation ou de mesures de contrôle permettent de restreindre au maximum l'atteinte causée aux libertés personnelles et donc de concevoir comme proportionnée la vidéosurveillance.

1668 La mise en pratique de ces précautions offre l'opportunité d'éviter que les droits fondamentaux soient restreints de manière injustifiée, extensivement assure que la preuve puisse être administrée au procès et exploitée selon la force qui lui sera reconnue.

ii. L'adoption ou la modification des bases légales en matière de vidéosurveillance dissuasive exercée par les autorités ou les particuliers et de la surveillance répressive opérée par les personnes privées

1669 La mise en œuvre et la réglementation des précautions que nous avons listées non-exhaustivement risquent de créer des législations fédérales ou cantonales éparses. C'est pourquoi la proposition d'une législation uniforme comprenant au minimum les principes de base pour la délimitation et l'organisation découlant de la vidéosurveillance paraîtrait cohérente.

1670 Dans le cadre de la vidéosurveillance opérée par les particuliers ou les autorités fédérales, il semble nécessaire – tout du moins – que la LPD instaure une ou plusieurs dispositions qui traitent explicitement et spécifiquement de la vidéosurveillance, corrélativement à l'art. 42 LIPAD/GE. Cette réglementation permettrait de clarifier la situation et d'éviter notamment, pour les particuliers, d'abuser de la vidéosurveillance principalement sur domaine privé.

1671 Concernant la vidéosurveillance dissuasive exercée par les autorités cantonales, les cantons sont seuls compétents pour légiférer sur le sujet, ce qui implique une grande diversité de normes. Alors que certains cantons doivent adopter une norme pour fonder la vidéosurveillance, d'autres ont déjà légiféré, de manière plus ou moins complète.

1672 Afin que les citoyens suisses et étrangers puissent se déplacer en divers lieux en ayant connaissance au minimum des principes généraux régissant la vidéosurveillance et le traitement subséquent des images, nous pensons que l'entrée en vigueur d'un concordat intercantonal sur la vidéosurveillance dissuasive serait une plus-value pour la sauvegarde des libertés personnelles et la garantie de la protection de la personnalité. Ainsi, grâce à un régime juridique égal dans tous les cantons, les citoyens pourraient appréhender correctement les droits et obligations imposés aux collectivités publiques.

1673 De notre avis, la vidéosurveillance dissuasive et/ou répressive doit donc faire l'objet d'une réforme afin de clarifier la situation juridique. Des bases légales précises et/ou harmonisées assureraient la sécurité juridique et garantiraient une protection adéquate des individus dans le cadre de la vidéosurveillance.

II. Les techniques de localisation

1674 Suite à l'accroissement des appareils permettant la mobilité des utilisateurs – appareils de type GSM, GPS ou de téléphonie mobile –, la traçabilité des individus est devenue opérante.

1675 Même lorsque nous ne sommes pas en communication à l'aide de notre téléphone mobile ou que nous n'utilisons pas notre navigateur GPS, ces appareils constituent des balises de positionnement.

1676 Dans le cadre de la procédure pénale, la géolocalisation est une technique d'interception utile à la neutralisation préventive ou répressive, notamment en permettant de relier une personne à une scène ou à une zone de crime. En contrepartie de cet avantage de traçabilité, la géolocalisation est une méthode intrusive dont l'utilisation peut potentiellement porter atteinte aux droits fondamentaux.

1677 La présente partie a pour dessein d'exposer deux technologies de localisation – par GPS et par téléphonie mobile –, leur cadre légal en procédure pénale et leur utilisation en tant que preuve.

A. Les principes généraux

1. La définition de la géolocalisation

1678 La géolocalisation est une technologie permettant de déterminer plus ou moins précisément la localisation spatio-temporelle d'un objet mobilier ou d'une personne à l'aide des coordonnées géographiques obtenues par le biais d'un système de positionnement satellite ou par le réseau de télécommunications.

1679 Les systèmes de téléphonie mobile permettant l'usage des natels, les systèmes mondiaux de navigation par satellite relié à un récepteur comme le GPS ou encore les terminaux de

correspondances électroniques servent à positionner les objets et/ou les individus[1325]. La localisation peut être une action volontaire de l'utilisateur d'un Smartphone, ordinateur ou récepteur GPS – par exemple, le service iCloud d'Apple permet de localiser son Iphone –, ou être réalisée sous réquisition de l'autorité compétente, notamment pour rechercher une personne suspecte ou disparue.

2. Le champ d'étude

a. Les services basés sur la localisation géographique

1680 Trois types de services peuvent fournir des informations sur la position spatio-temporelle d'un individu: les systèmes de navigation par satellite, les systèmes de télécommunication mobile et les terminaux informatiques. Nous traiterons ici des deux premiers, la géolocalisation par l'adresse IP faisant l'objet des preuves issues des techniques informatiques[1326].

1681 Les systèmes mondiaux de navigation par satellite, dont fait partie le GPS, donnent les positions de l'appareil transmetteur dans un rayon de quelques dizaines de mètres[1327]. Ce type de système, connu principalement dans le cadre de la navigation automobile, avait à l'origine pour but de positionner son utilisateur et de l'aider à se déplacer. Aujourd'hui, il sert notamment au secours en cas d'urgence ou à la recherche d'objets volés, d'animaux ou de personnes. Le GPS est donc utilisé comme système de localisation pure, mais peut également permettre de retracer *a posteriori* les déplacements d'un véhicule ou servir comme élément de filature[1328].

1682 Les systèmes de télécommunication mobile localisent le téléphone portable émetteur ou récepteur. En premier lieu nécessaires pour établir les communications, les antennes relais ont rapidement démontré leur potentiel pour les autorités dans le cadre des recherches de personnes.

[1325] BAUER, FREYNET, p. 64; BONDALLAZ, protection des personnes, p. 31-32; DODEL, HÄUPLER, p. 1.

[1326] Infra Partie II, Chapitre 3, III, A, 3, c, ii, n° 2054 ss; Infra Partie II, Chapitre 3, III, A, 4, b, n° 2104 ss; Infra Partie II, Chapitre 3, III, A, 5, b, n° 2142 ss.

[1327] BONDALLAZ, protection des personnes, p. 31; OCDE, p. 184-191. Infra Partie II, Chapitre 3, II, B, 1, n° 1688-1691.

[1328] BIRRER, TERRETTAZ-ZUFFEREY, p. 482; CORNU, p. 248; LANGLOIS, BRODEUR, p. 76.

b. La géolocalisation en Suisse via la téléphonie mobile et les installations GPS

1683 En Suisse, la géolocalisation à l'aide des systèmes de télécommunication mobile est la plus répandue. Les appareils GPS sont plus rarement exploités[1329].

1684 L'exploitation plus fréquente du positionnement spatio-temporel par téléphonie mobile s'explique par son lien étroit avec la surveillance des télécommunications. Lorsque les fournisseurs de services de télécommunication effectuent une surveillance en temps réel ou rétroactive, la détermination et la transmission simultanée ou périodique de l'identification cellulaire (Cell ID) (art. 16 let. b OSCPT), la position et la direction d'émission de l'antenne relais (art. 16 let. d ch. 3 OSCPT) font parties des données transmises à l'autorité pénale. La surveillance des télécommunications étant fréquente, dès qu'elle concerne un raccordement de téléphonie mobile, les données relatives à l'antenne relais (BTS), soit les données de positionnement, sont connues de l'autorité pénale.

1685 Les données de localisation issues de la navigation GPS ne dépendent en revanche jamais de la surveillance des télécommunications. Il s'agit d'une surveillance spécifique, raison pour laquelle son utilisation est moins fréquente.

c. La localisation ou le suivi spatio-temporel

1686 Qu'elles dépendent de la téléphonie mobile ou d'un récepteur GPS, les données de localisation servent de méthode de surveillance judiciaire, plus spécifiquement de surveillance spatio-temporelle. En fournissant des indications sur la localisation du support, ces données permettent extensivement d'obtenir le positionnement de son utilisateur. Grâce aux ordinateurs, il est possible de géoréférencer toutes ces données spatio-temporelles afin de reconstituer les déplacements d'un individu, de situer les lieux de commission d'une infraction s'étendant dans l'espace ou de signaler en temps réel les allées et venues d'une personne surveillée.

1687 En outre, les données de localisation peuvent être combinées avec d'autres informations permettant de surveiller ou d'élucider le déroulement des faits. Par exemple, en ce qui concerne le GPS, les temps d'arrêts ou encore la vitesse sont des informations qui peuvent

[1329] BIRRER, TERRETTAZ-ZUFFEREY, p. 482; MÉTILLE, Thèse, p. 68.

être utiles selon la nature de l'infraction considérée ou si le temps de déplacement a son importance pour élucider les faits[1330].

1688 La téléphonie mobile et le GPS sont donc la source d'un nombre considérable d'informations permettant de déterminer la position géographique d'un individu. Ainsi, la consultation, la surveillance et la vérification des données spatio-temporelles peuvent permettre notamment de protéger certaines personnes – nous pensons ici à la surveillance à l'aide d'un appareil GPS des personnes atteintes de la maladie d'Alzheimer ou d'un trouble psychologique –, de localiser immédiatement l'emplacement d'un appelant en cas d'urgence, de soutenir la lutte contre la délinquance ou encore de lutter contre le terrorisme. *De facto*, les systèmes de géolocalisation participent à la mise en place d'un réseau pouvant amener des informations précieuses lors d'une enquête pénale ou pour rechercher des personnes disparues[1331].

B. Le contexte technique

1. La localisation à l'aide de la technologie GPS

a. Le système de navigation par satellite et les données fournies

1689 Les signaux émis par les satellites des constellations des systèmes mondiaux de navigation (GPS, GLONASS ou GALILEO) contiennent un message d'identification qui indique quel est le satellite émetteur, quelle est l'heure exacte d'émission et où sont positionnés sur le plan orbital tous les satellites exploités.

1690 La réception des signaux émis par au moins trois satellites permet le positionnement du récepteur dans l'espace à deux dimensions – longitude et latitude – grâce à la distance calculée à l'aide de la position des satellites et du temps que met un signal pour parvenir audit satellite[1332]. Dès lors que les horloges des récepteurs ne sont pas aussi précises que celles des satellites, le décalage de temps peut apporter quelques imprécisions, il est alors préférable de calculer la position du récepteur à l'aide de quatre satellites[1333].

[1330] Infra Partie II, Chapitre 3, II, B, 1, b, ii, n° 1697-1702; Infra Partie II, Chapitre 3, II, E, 1, c, iii, n° 1807-1809.

[1331] OFCOM, Localisation, p. 13 et 16; OOSTERLINK, p. 95-101. Infra Partie II, Chapitre 3, II, D, n° 1780-1781.

[1332] ANDREANI, p. 25; BIRRER, TERRETTAZ-ZUFFEREY, p. 485; DODEL, HÄUPLER, p. 5, 47 et 316-317; MÉTILLE, Thèse, p. 68-69.

[1333] DODEL, HÄUPLER, p. 47 et 318; OOSTERLINK, p. 89.

1691 La précision fournie par les données de positionnement est relativement fiable permettant de localiser le récepteur et, par prolongement, l'utilisateur dans le cadre de la recherche policière. Néanmoins, un certain nombre d'erreurs inhérentes aux systèmes de navigation dont il faut tenir compte existent[1334].

1692 L'exploitation des systèmes de navigation par satellites permet donc de positionner à un moment précis un récepteur GPS. En revanche, ils n'ont pas pour fonction de fournir des indications sur le déplacement d'un récepteur. C'est pourquoi, la combinaison à un système de communication est nécessaire afin d'avoir une vue directe sur le positionnement en temps réel[1335]. Si un tel système n'est pas mis en place, seuls les enregistrements ou historiques de l'appareillage GPS pourront être exploités dans le dessein d'obtenir une information sur les trajets effectués. Les enregistrements sur un serveur externe au GPS ou l'historique stocké dans la mémoire interne de l'appareil, ainsi que les enregistrements ou les historiques du récepteur GPS, fournissent les données relatives à l'heure, à la vitesse, au positionnement géographique – longitude et latitude – du véhicule surveillé[1336].

1693 Dans l'hypothèse où la voiture du suspect n'est pas munie d'un appareil de géo-positionnement, un traceur GPS peut être discrètement fixé sur le véhicule. Cette méthode facilite la filature. Ainsi, l'enquêteur connaît en permanence le lieu où se trouve le véhicule, où il se dirige et s'il est à l'arrêt.

1694 Relevons encore qu'aujourd'hui de nombreux utilisateurs de téléphonie mobile ont un Smartphone muni d'un module GPS qui permet d'avoir un système de réception. Il est ainsi possible de localiser le téléphone *via* les systèmes de navigation par satellite.

b. Le cas particulier des boîtes noires et du système ISA

i. Intelligent Speed Assistance

1695 Depuis quelques années, les assureurs automobiles proposent de doter les véhicules d'une unité de communication entièrement automatisée, appelée plus communément boîte noire. Ce système permet de collecter les données kilométriques, les trajets effectués, les

[1334] Infra Partie II, Chapitre 3, II, E, 2, b et c, n° 1837 ss et 1851 ss.

[1335] A ce sujet: http://www.geogeny.ch [consulté le 08.05.2016].

[1336] BIRRER, TERRETTAZ-ZUFFEREY, p. 486.

informations relatives au comportement de conduite soit en temps réel, soit passivement en se connectant directement à l'appareil[1337].

1696 Dans la même optique, à l'aide d'une boîte noire, le système d'assistance ISA – Intelligent Speed Assistance – développé par les australiens prévient et maîtrise la problématique des excès de vitesse. Il s'agit d'un système qui incite le conducteur ou l'oblige à respecter les limitations de vitesse.

1697 Pour fonctionner, le système ISA doit être positionné dans un véhicule. Un GPS détermine avec précision la position du véhicule grâce au signal satellite. Une banque de données recense la totalité des tronçons routiers avec les vitesses maximales autorisées. Grâce à une carte digitale, ISA connaît le régime de vitesse en vigueur et peut le comparer avec les données sur la position du véhicule. L'information obtenue par ISA est alors envoyée au conducteur et/ou à la voiture. Le système peut soit alerter l'automobiliste que sa vitesse est trop élevée, soit la réduire automatiquement en créant une contre-pression sur l'accélérateur rendant difficile l'accélération ou empêcher directement l'excès de vitesse[1338].

ii. Le programme Via sicura

1698 Dans le cadre du programme Via sicura[1339], l'OFROU, désireux de surveiller les chauffards, propose d'employer un enregistreur de données basé sur les systèmes de boîtes noires et ISA sans la fonctionnalité de régulation de vitesse, mais avec un enregistrement des informations relatives à la vitesse.

1699 La modification de la Loi sur la circulation routière (LCR) a été acceptée par les Chambres fédérales le 15 juin 2012. Concernant l'utilisation des boîtes noires, l'entrée en vigueur de l'art. 17a du projet modifiant la LCR (P-LCR) était prévue dès l'année 2015, mais se trouve repoussée en 2017 au plus tôt[1340].

[1337] A ce sujet: PFPDT, *Explication concernant les systèmes "Pay you drive" (PAYD) et l'utilisation de "boîtes noires" dans les véhicules automobiles*, disponible sur: http://www.edoeb.admin.ch [consulté le 08.05.2016]; http://www.masternaut.com [consulté le 08.05.2016].

[1338] A ce sujet: http://www.isaweb.be [consulté le 08.05.2016].

[1339] Message, Via sicura, p. 7703 ss.

[1340] DETEC, *Via Sicura – Feuille d'information*, Berne 20 janvier 2015, disponible sur: http://www.astra.admin.ch [consulté le 08.05.2016].

1700 L'art. 17a P-LCR prévoit que:

> [1] *Si le permis de conduire a été retiré en vertu de l'art. 16b, al. 2, let. e ou f, 16c, al. 2, let. c ou d, ou 16d, al. 1, let. c, pour cause de dépassement de la vitesse maximale autorisée ou de vitesse inadaptée aux conditions de circulation, la personne concernée ne peut conduire, durant cinq ans après la restitution du permis, que des véhicules munis d'un enregistreur de données.*
> [2] *Dans des cas dûment motivés, l'autorité peut autoriser la conduite de véhicules non munis d'un enregistreur de données.*
> [3] *Si la personne concernée conduit un véhicule non muni d'un enregistreur de données, le permis de conduire lui sera retiré pour une durée appropriée.*
> [4] *Le Conseil fédéral édicte des prescriptions concernant les exigences requises pour l'appareil et le contrôle de ce dernier.*

1701 Actuellement, un conducteur ayant commis un excès de vitesse grave ou ayant plusieurs fois transgressé les prescriptions en matière de vitesse se voit retirer l'autorisation de conduire. Une fois la période de retrait terminée, aucune surveillance particulière n'est prévue durant le délai d'épreuve.

1702 Pour éviter les récidives et pour protéger au mieux la collectivité, il convient de fixer un délai d'épreuve avec surveillance aux "chauffards"[1341]. Ainsi, les personnes visées par l'art. 17a al. 1 P-LCR ne peuvent conduire qu'un véhicule muni d'un enregistreur de données.

1703 La surveillance des excès de vitesse à l'aide de l'équipement de géopositionnement a – avant tout – un effet psychologique, extensivement préventif, puisque le conducteur est confronté quotidiennement aux données enregistrées[1342]. Si l'effet dissuasif de l'appareil ne conditionne pas l'attitude d'un conducteur et qu'il commet une nouvelle infraction à la LCR, les données obtenues peuvent être utilisées comme moyen de preuve afin de le sanctionner à nouveau.

2. La localisation lors d'une surveillance de la télécommunication mobile

1704 Nous l'avions relevé à l'aune de la surveillance des télécommunications, les diverses informations fournies par les téléphones mobiles aident les services de police et la justice

[1341] Message, Via sicura, p. 7726.

[1342] DETEC, p. 30.

pour mener à bien une enquête ou une procédure pénale[1343]. Nous nous axons à présent sur la localisation géographique à l'aide des réseaux de télécommunication mobile.

a. La localisation à l'aide du réseau de téléphonie mobile

1705 La téléphonie mobile fonctionne à l'aide d'ondes radioélectriques entre une antenne relais et un téléphone. Deux grands standards de systèmes mobiles existent: l'IS41 d'origine américaine et le GSM/UMTS. Ce dernier étant actuellement le standard en Europe et est donc exploité en Suisse, il fait l'objet de notre analyse.

i. Les systèmes de téléphonie

1706 Le GSM – Global System for Mobile Communications – est un système de téléphonie mobile cellulaire. La zone desservie par le fournisseur de services de télécommunication est divisée en cellules alimentées par une station de base ou antenne relais[1344]. Les antennes relais couvrent donc une certaine parcelle du territoire allant de 100 mètres à 10 kilomètres. Une ou plusieurs fréquences d'émission spécifiques sont attribuées à chaque cellule et réutilisées que par des cellules éloignées afin d'éviter les perturbations.

1707 Pour établir une communication, le téléphone mobile crée une liaison radio avec l'antenne relais. Chacune d'entre-elles est reliée à une unité centrale par câble ou parabole qui traite les informations entrante ou sortante du téléphone portable et enregistre l'antenne qui est activée par l'utilisation du mobile. Si l'utilisateur se déplace vers la limite de la cellule, la première antenne transfère automatiquement la communication à la seconde pour éviter les interférences et les coupures.

1708 Les systèmes dits de troisième génération – Universal Mobile Telecommunications System – UMTS – ou Long Term Evolution – LTE – fonctionnent selon le même procédé.

1709 Ainsi, dès qu'une communication est réalisée à l'aide d'un natel ou qu'un SMS est envoyé, la référence spatiale de l'antenne, la date, l'heure et la durée de conversation sont conservées pour une durée de six mois et sont disponibles aux autorités répressives[1345]. En analysant les

[1343] Supra Partie II, Chapitre 3, I, A, 3 et 4, n° 1235 ss et 1253 ss.

[1344] BIRRER, TERRETTAZ-ZUFFEREY, p. 484; CARTIER, p. 201-202; OFEFP, p. 11.

[1345] HANSJAKOB, Antennensuchläufen, n° 2-3. A ce sujet, voir également: Infra Partie II, Chapitre 3, II, C, 2, a, ii, b), n° 1760 et 1768.

données enregistrées, il est alors possible de connaître la ou les antennes qui se sont activées et ainsi localiser dans le temps l'utilisateur de manière plus ou moins précise. En l'absence de communication, aucune donnée sur l'emplacement des antennes activées par le téléphone mobile n'existe[1346].

1710 En sus de l'utilisation des signaux émis par un téléphone mobile et corrélativement à ce qui prévaut pour le traceur GPS positionné sur un véhicule, une balise émettant des ondes radios peut également être placée sur un suspect ou un véhicule afin de le suivre et/ou de le positionner.

ii. La localisation des téléphones portables à l'aide des antennes relais

1711 Diverses technologies utilisent le GSM, extensivement la localisation par antennes relais, pour identifier la position d'un téléphone, notamment:

- La Cell ID – identification de cellule – est la technologie la plus simple, mais la moins précise puisqu'il ne s'agit que de localiser la cellule et non le téléphone. Elle dépend étroitement du nombre d'antennes relais proches de l'appareil de téléphonie, de la grandeur de la cellule couverte et de l'environnement rural ou urbain.

  Lorsqu'un utilisateur se trouve dans une zone couverte par le réseau, il se connecte automatiquement à une antenne relais. Le téléphone transmet les données IMEI permettant à la carte SIM de s'identifier sur le réseau.

  En quelques secondes, il est possible de connaître de manière plus ou moins vaste la localisation du téléphone mobile, extensivement de son utilisateur.

  Cette technique ne nécessite pas que le téléphone soit en permanence allumé ou dans une zone de couverture GSM. Il est en effet possible de récupérer les identifiants sur une antenne relais à laquelle le mobile s'est connecté sans qu'il le soit encore et ainsi permettre la surveillance rétroactive.

- La triangulation avec l'aide de l'opérateur ou le *Net Monitoring* – contrôle du réseau – emploie le croisement de données issues de trois antennes relais ce qui accroît la précision, mais cette technique est peu efficace en zone urbaine dès lors qu'elle nécessite un environnement libre d'obstacles.

  Il suffit que le téléphone soit allumé en veille pour que la localisation soit possible. Cependant, l'installation au préalable d'un logiciel sur la carte SIM est nécessaire.

[1346] BIRRER, TERRETTAZ-ZUFFEREY, p. 485; CARTIER, p. 214; HANSJAKOB, Antennensuchläufen, n° 3.

Cette technologie est d'ailleurs largement employée par les hackers qui activent la fonction *Net Monitoring* se trouvant d'office mais inactive sur les mobiles récents pour positionner un individu.

Pour éviter la triangulation, l'utilisateur du téléphone mobile n'a pas d'autre choix que d'enlever sa carte SIM après chaque communication, voire d'utiliser plusieurs puces pour éviter le pistage[1347].

Découlant de ce principe de triangulation et de l'exploitation d'une application sur la carte SIM, la technologie AOA – Angle of Arrival – emploie la force du signal des antennes couvrant un champ directionnel d'environ 120° sise sur un mât[1348]. En comparant les amplitudes, il est possible d'établir un angle de 10°-15° pour chacune des trois antennes. La position en deux dimensions peut être ainsi fournie avec une précision de 125 mètres à 4 kilomètres[1349].

- EOTD – Enhanced Observed Time Difference – utilise le temps écoulé entre l'émission par le téléphone portable d'un signal aux stations mobiles et la réception en retour du signal émis par lesdites stations, trois ou plus[1350]. Un serveur externe estime à l'aide du temps écoulé la distance de l'appareil par rapport à l'antenne et positionne ainsi le téléphone avec un taux d'erreur de 50 à 150 mètres.

  Cette technologie demande la disposition géographique précise des antennes sans quoi le taux d'approximation de la localisation s'accentue.

  Sur le même procédé, la technologie TOA – Time of Arrival – et TODA – Time Difference of Arrival – prend en considération la triangulation par relevé de la distance entre le terminal et le téléphone mobile en mesurant le temps d'arrivée du signal entre trois antennes relais et le téléphone. L'intersection des cercles de transmission fournit le positionnement du natel.

  Le défaut principal de ces méthodes de localisation est l'influence importante de la réflexion des ondes (bâtiments, montagnes, etc.) qui empêche de calculer correctement le positionnement dans certaines zones.

1712 Il existe de nombreuses autres technologies permettant de positionner un téléphone mobile avec une approximation plus ou moins importante. En toute hypothèse, la localisation à

[1347] BUQUET, p. 362; RIKLIN, Strafprozessordnung, art. 280 N 3.

[1348] HANSJAKOB, Antennensuchläufen, n° 1.

[1349] CARTIER, p. 207; KÜPPER, p. 158.

[1350] BUQUET, p. 363; DUHEN, p. 142.

l'aide de la téléphonie mobile reste en deçà de ce que nous pouvons obtenir à l'aide de la localisation satellite[1351].

b. Le cas particulier de la recherche par champ d'antennes ou balayage d'antennes

1713 Lorsqu'un téléphone portable entre dans la zone d'une antenne relais, il communique immédiatement avec elle afin de pouvoir émettre ou recevoir des appels ou des messages. La recherche par champ d'antennes est une recherche rétroactive de toutes les communications effectuées par la téléphonie mobile à un endroit précis et durant un laps de temps déterminé (art. 16 let. e OSCPT).

1714 En règle générale, lors d'une surveillance à l'aide de la téléphonie mobile, les autorités pénales ciblent un numéro ou un utilisateur déterminé. Grâce à la recherche par champ d'antennes, il est possible d'analyser toutes les données – liste des numéros ayant activé une antenne – d'une ou de plusieurs antennes relais, après avoir déterminé la cellule concernée par le lieu fourni par l'autorité pénale[1352]. Ce type de recherches élargies des téléphones ayant été en contact avec une antenne relais est largement bénéfique pour l'administration de la justice[1353].

C. Le cadre légal

1. Les droits fondamentaux, les libertés et leur protection

1715 Corrélativement aux autres mesures de surveillance secrète précédemment analysées, les techniques de localisation mettent en péril la liberté personnelle (art. 10 al. 2 Cst), le droit au respect de la sphère privée (art. 8 CEDH, art. 17 Pacte II et art. 13 al. 1 Cst) et le droit d'être protégé contre l'emploi abusif de ses données personnelles (art. 13 al. 2 Cst)[1354].

1716 En revanche, contrairement à la vidéosurveillance avec enregistrement ou à la surveillance des télécommunications, la localisation d'une personne ou d'un objet ne comporte pas

[1351] CARTIER, p. 212; KÜPPER, p. 175.

[1352] HANSJAKOB, Antennensuchläufen, n° 2 et 4; HEINIGER, n° 36.

[1353] Infra Partie II, Chapitre 3, II, E, 1, c, iv, n° 1813-1815.

[1354] Supra Partie II, Chapitre 3, I, A, 2, a, i, n° 1116 ss; Supra Partie II, Chapitre 3, I, B, 2, a, i, n° 1451 ss.

nécessairement une atteinte à la sphère privée ou secrète des individus surveillés ou, tout du moins, l'atteinte est qualifiée de légère[1355].

1717 La Cour européenne des droits de l'homme a eu l'occasion, dans l'Affaire *Uzun c. Allemagne*, de se déterminer sur la violation de l'art. 8 CEDH, lors de l'exploitation des données GPS pour localiser un individu. Le constat réalisé par la Cour vaut également pour la localisation de la téléphonie mobile à ceci près que le secret des télécommunications protège également les renseignements ou données accessoires dont font parties les données de positionnement de téléphonie mobile[1356]. Leur transmission constitue toutefois une atteinte moins grave aux droits fondamentaux que l'interception ou l'enregistrement de la correspondance.

a. Les principes pertinents

1718 La Cour européenne des droits de l'homme s'est déterminée à plusieurs reprises sur l'étendue reconnue à la protection de la vie privée[1357].

1719 L'art. 8 CEDH protège notamment le droit à l'identité et au développement personnel ainsi que le droit de nouer des relations avec des tiers. Le terme "privée" ne doit pas s'entendre dans un sens strict. Il n'est pas exclu que des éléments de la vie privée puissent être protégés lorsqu'ils ressortent d'un contexte public.

1720 Lorsqu'il s'agit de déterminer si la vie privée est touchée en dehors du domicile ou des locaux privés de la personne surveillée, la Cour européenne des droits de l'homme fait une évaluation au cas par cas. Un certain nombre d'éléments peuvent entrer en considération.

1721 Il est notamment intéressant de déterminer ce qu'un individu est en droit d'attendre quant au respect de sa vie privée lorsqu'il se promène dans la rue[1358]. En effet, un individu qui se

---

[1355] Message, CPP, p. 1234.

[1356] Supra Partie II, Chapitre 3, I, A, 2, a, n° 1116 ss.

[1357] CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 56; CourEDH, Affaire *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, 44647/98, § 57; CourEDH, Affaire *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, 63737/00, § 36; CourEDH, Affaire *von Hannover c. Allemagne*, arrêt du 24 juin 2004, 59320/00, § 50; CourEDH, Affaire *Reklos et Davourlis c. Grèce*, arrêt du 15 janvier 2009, 1234/05, § 35-36.

[1358] ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 57; CourEDH, Affaire *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, 44647/98, § 58-63; CourEDH, Affaire *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, 63737/00, § 37-38.

promène sur domaine public doit s'attendre à être vu, extensivement à être observé par une autorité.

1722 En revanche, l'enregistrement systématique ou permanent de données, même obtenues en zone publique, permet le traitement et l'utilisation des données personnelles[1359]. Dans de telles circonstances, des considérations liées à la vie privée entrent en ligne de compte[1360].

1723 En outre, la Cour prend en considération la nature de la donnée recueillie qui doit être personnelle et concerner un individu précis, ainsi que l'utilisation qui en est faite. En effet, lorsque l'autorité pénale emploie la donnée en la reliant à d'autres informations pour identifier une personne ou élucider un fait en lien avec cette personne, il s'agit d'un traitement de données personnelles qui constitue une ingérence dans le respect de la vie privée[1361].

b. Le respect de la vie privée en cas de localisation GPS

1724 La localisation de la téléphonie mobile est directement liée aux données accessoires obtenues lors d'une surveillance des télécommunications[1362]. Nous nous intéressons donc ici plus particulièrement au positionnement effectué à l'aide des données GPS en ajoutant quelques détails concernant la téléphonie mobile.

1725 Dans l'affaire *Uzun c. Allemagne*, la Cour de Strasbourg a appliqué les principes susmentionnés pour se déterminer sur l'ingérence dans le respect de la sphère privée que peut causer l'utilisation d'un système de localisation par satellite.

1726 Le premier élément que la Cour a examiné est celui de l'individualité de la donnée. La localisation par GPS est autorisée à l'égard du prévenu et dans certaines circonstances à l'égard de tiers[1363]. En cas de surveillance d'un local ou d'un véhicule d'un tiers, ce qui est

[1359] CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65-66; CourEDH, Affaire *Rotaru c. Roumanie*, arrêt du 4 mai 2000, 28341/95, § 43-44; CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 57; CourEDH, Affaire *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, 44647/98, § 59; CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 65-66; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 64.

[1360] CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 59-60; CourEDH, Affaire *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, 63737/00, § 40-41.

[1361] CourEDH, Affaire *P.G et J.H c. Royaume-Uni*, arrêt du 25 septembre 2001, 44787/98, § 59-60; CourEDH, Affaire *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, 63737/00, § 38.

[1362] Supra Partie II, Chapitre 3, I, A, 2, a, n° 1116 ss.

[1363] Infra Partie II, Chapitre 3, II, C, 2, a, i, n° 1741.

déterminant, c'est de savoir qui l'autorité d'enquête désire surveiller et non pas qui est le propriétaire du bien. Ainsi, il est possible de déterminer quelle est la personne dont la vie privée est touchée[1364].

1727 La Cour relève également que la surveillance au moyen de la localisation GPS par une autorité pénale amène immanquablement le recueil systématique et permanent – durant la période de surveillance – des données de déplacement de la personne. Vraisemblablement, ces informations sont en outre enregistrées afin de permettre de suivre l'individu ou de lier le positionnement à un moment donné dans un lieu donné avec la réalisation d'une infraction[1365].

1728 Ainsi, au regard de l'art. 8 CEDH, la localisation par GPS employée comme preuve pénale, soit la surveillance d'une personne déterminée couplée avec le traitement et l'utilisation des données atteint au respect de la vie privée[1366]. L'utilisation des informations émises par les antennes relais pour déterminer le positionnement d'un téléphone mobile étant également un service de localisation, le constat effectué par la Cour européenne des droits de l'homme concernant le GPS vaut par analogie à la téléphonie mobile dans le cadre de la géolocalisation.

c. La nature de l'atteinte à la vie privée

1729 Concernant la gravité de l'atteinte, la Cour européenne distingue la surveillance par GPS – par analogie, à l'aide de la téléphonie mobile dans la stricte circonstance où seule la donnée de positionnement est fournie – et les autres méthodes de surveillances visuelles ou acoustiques.

1730 De par sa nature, la géolocalisation est moins intrusive dès lors qu'elle ne fournit pas d'informations sur le comportement, les opinons ou les sentiments de la personne surveillée[1367]. Néanmoins, en cas de traitement et d'utilisation des données obtenues à l'aide d'une surveillance GPS, l'atteinte à la vie privée est – au minimum – légère.

[1364] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 49.

[1365] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 51; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 65.

[1366] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05.

[1367] ATF 130 II 425, 447-448; TF 1P_51/2007 du 24 septembre 2007, c. 3.5.4; TF 2C_116/2011 du 29 août 2011, c. 8.4; CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 52 et 72; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 65; BSK-StPO-KATZENSTEIN, EUGSTER, art. 280 N 35 ss;CR-

1731 Par conséquent, l'ingérence à la vie privée doit être justifiée.

2. La justification de l'ingérence

a. L'existence d'une loi et la prévisibilité de la norme

1732 Dans le contexte de la surveillance des télécommunications, la Cour européenne a déterminé des critères. La loi doit définir:

- la nature des infractions susceptibles de donner lieu à un mandat d'interception;
- les personnes susceptibles d'être mises sur écoute;
- la durée maximale de l'exécution;
- la procédure de mise en œuvre, d'utilisation et de conservation des données;
- les précautions à prendre en cas de communication des données; et,
- les circonstances pour l'effacement ou la destruction des données.

1733 Ces quelques éléments doivent permettre de se déterminer sur la suffisance en termes de prévisibilité de la loi et sur l'existence de garanties adéquates contre les abus[1368].

1734 Néanmoins, ces critères stricts s'appliquent exclusivement à la surveillance des télécommunications, extensivement à la localisation par téléphonie mobile ou à la recherche par champ d'antennes[1369].

1735 Pour qu'une protection adéquate de la vie privée soit reconnue en cas de surveillance par la géolocalisation au moyen d'un système GPS, la Cour européenne se base sur les principes généraux. L'ingérence doit être prévue par une loi et être suffisamment prévisible. Afin de déterminer la prévisibilité de la norme, il faut apprécier l'existence de garantie adéquate en

---

CPP-BACHER, ZUFFEREY, art. 280 N 14; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 270; Message, CPP, p. 1234.

[1368] CourEDH, Affaire *Weber et Saravia c. Allemagne*, arrêt du 29 juin 2006, 54934/00, § 95; CourEDH, Affaire *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie*, arrêt du 28 juin 2007, 62540/00, § 76; CourEDH, Affaire *Liberty et autres c. Royaume-Uni*, arrêt du 1er juillet 2008, 58243/00, § 62; CourEDH, Affaire *Iordachi et autres c. Moldova*, arrêt du 10 février 2009, 25198/02, § 39; CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 65-66; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 68.

[1369] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 65-66; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 68.

fonction de la nature, de l'étendue et de la durée de la surveillance. En outre, les conditions de mise en œuvre, les autorités compétentes pour les ordonner et les exécuter, et les recours fournis par le droit interne sont des éléments à considérer.

i. La procédure de mise sous surveillance au moyen des systèmes de navigation par satellite

1736 Avant l'entrée en vigueur du CPP, la surveillance par GPS de la position d'un véhicule sur le domaine public était dépourvue de base légale à défaut d'entrer dans le champ d'application de la LSCPT[1370]. Une preuve issue de ce procédé était dès lors illégale et donc – en principe – irrecevable[1371]. Cette lacune est aujourd'hui comblée.

a) La prévisibilité de la loi

1737 L'art. 280 let. c CPP règlemente l'utilisation d'appareils techniques qui ne sont ni visuels ni acoustiques et qui permettent de localiser une personne ou une chose.

1738 La surveillance par GPS ne constituant ni une surveillance visuelle ni acoustique et permettant, à l'aide des données stockées ou enregistrées sur un serveur, de géopositionner ou d'établir des profils de déplacement d'une personne, d'un véhicule ou d'un objet[1372], cette surveillance est couverte par l'art. 280 let. c CPP.

1739 Il ressort donc clairement du libellé de la loi que le moyen technique de localisation par GPS est prévu comme moyen de contrainte[1373]. L'exigence de prévisibilité est sur ce point satisfaite.

b) La procédure et les garanties contre les abus

1740 Au regard de la jurisprudence de la Cour européenne des droits de l'homme[1374], la surveillance par GPS doit remplir un certain nombre de conditions pour admettre comme

---

[1370] TF 1P_51/2007 du 24 septembre 2007, c 3.4 et 3.5; VETTERLI, p. 84-85.

[1371] ATF 131 I 272, 281; TF 1P_51/2007 du 24 septembre 2007, c. 3.5, plus spécifiquement c. 3.5.6; CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 60.

[1372] BSK-StPO-KATZENSTEIN, EUGSTER, art. 280 N 37; Message, CPP, p. 1234; RÉMY, p. 112; PITTELOUD, p. 457; RUCKSTUHL, DITTMANN, ARNOLD, p. 271; SCHMID, Praxiskommentar, art. 280 N 10; StPO-HANSJAKOB, art. 280 N 8.

[1373] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 67-68.

justifiée l'ingérence. La loi doit notamment renfermer des garanties suffisantes et effectives contre les abus.

1741 Aux fins de ces garanties et pour protéger au mieux la vie privée, la Cour énumère un certain nombre d'éléments. Le droit interne doit contenir l'indication d'une durée ou tout du moins la durée de surveillance doit rester proportionnée aux circonstances. Les motifs requis pour ordonner une surveillance doivent être délimités, notamment en indiquant qui peut être surveillé, dans quelles circonstances – crime, délit, liste exhaustive d'infractions, etc. – une surveillance par GPS peut être mise en œuvre, et qui a la compétence de donner l'ordre de localiser un individu en employant les systèmes de navigation par satellite. Afin d'avoir une protection suffisante contre l'arbitraire, la Cour rappelle qu'un contrôle judiciaire subséquent à l'ordre de mise sous surveillance est adéquat et préférable. Enfin, la possibilité d'écarter les éléments de preuve inutiles ou obtenus illégalement ainsi que le recours subsidiaire à la méthode de surveillance permettent d'affirmer que l'ingérence dans l'exercice du droit à la vie privée est prévue par la loi.

1742 Quant aux conditions pour ordonner la mesure de surveillance par GPS, la durée d'un tel procédé, le traitement des informations recueillies, l'utilisation des découvertes fortuites, la levée de la surveillance et la communication aux personnes concernées par cette méthode, elles sont similaires à celles applicables pour la vidéosurveillance du domaine privée ou secret effectuée par les autorités (art. 281 CPP, et art. 269 et 274 al. 5 phr. 1 CPP par analogie)[1375]. Au surplus, les articles concernant la surveillance de la correspondance par poste et télécommunication sont applicables (art. 269 ss CPP *cum* 281 al. 4 CPP)[1376].

1743 Mentionnons encore que le champ d'application des art. 280-281 CPP se limite à la surveillance en temps réel à l'aide du système de localisation par satellite dans le cadre de la poursuite pénale.

1744 Par conséquent, nous pouvons affirmer que le Code de procédure pénale suisse subordonne l'utilisation de la mesure de surveillance au respect de conditions légales strictes assurant une garantie adéquate contre les abus.

[1374] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 69-73; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 68.

[1375] Supra Partie II, Chapitre 3, I, B, 2, c, ii, d), n° 1553 ss.

[1376] Supra Partie II, Chapitre 3, I, A, 2, c, n° 1142 ss.

c) La surveillance par GPS à but préventif et la surveillance rétroactive

1745 L'exploitation à but préventif de la surveillance par GPS relève des normes du droit cantonal sur la police. Par manque de législation, actuellement de nombreux cantons ne peuvent donc pas l'exercer[1377].

1746 Quant aux données GPS qui ne font pas l'objet d'une surveillance en temps réel, les normes relatives aux perquisitions (art. 244-248 CPP), séquestres (art. 263-268 CPP) et à l'obligation de dépôt (art. 265 CPP) sont applicables[1378]. En effet, il s'agit alors d'obtenir les informations grâce aux enregistrements des déplacements sur un serveur ou à l'aide de l'historique de la mémoire cache de l'appareil de navigation, ce qui sort de l'utilisation pure d'un dispositif technique permettant de localiser un individu.

d) Les divergences entre la surveillance par GPS et l'observation

1747 En cas de filature, l'art. 280 CPP n'est pas pertinent. En effet, l'art. 282 CPP concernant l'observation est plus spécial.

1748 Dans les faits, qu'une autorité pénale suive un véhicule directement sans recourir à un dispositif technique ou surveille à distance plus éloignée ce même véhicule à l'aide d'un système GPS, l'atteinte aux droits fondamentaux est similaire. Dans certaines circonstances, la pose d'une balise GPS est même moins intrusive que l'observation puisqu'elle ne permet pas de visualiser les faits[1379].

1749 En pratique, les deux situations sont donc quasiment identiques et permettent d'obtenir le même résultat, à condition que la filature s'exécute discrètement.

1750 Pourtant, alors que l'observation nécessite une autorisation si elle dure plus d'un mois, le tribunal des mesures de contrainte doit approuver la localisation par GPS. Il est difficile de comprendre le raisonnement du législateur sur ce point vu la ressemblance pratique des deux mesures. Il n'en reste pas moins qu'il a clairement voulu différencier les deux mesures et instaurer un régime plus strict lors de l'utilisation d'un appareil de localisation dans un but probatoire – par exemple, lors de la fixation secrète d'un dispositif GPS sur le véhicule

[1377] Supra Partie II, Chapitre 3, I, A, 4, c, ii, c), n° 1362-1372.

[1378] Infra Partie II, Chapitre 3, III, A, 3, c, iii, n° 2060 ss.

[1379] GISLER, p. 87-90; VEST, p. 668-670; ZALUNARDO-WALSER, p. 51-52.

d'un suspect – afin d'analyser et/ou de conserver les déplacements d'une personne surveillée[1380].

ii. La procédure de mise sous surveillance au moyen des systèmes d'antennes relais

a) La différence entre les dispositifs employant les systèmes mondiaux de navigation par satellite et le système de téléphonie

1751 L'art. 280 let. c CPP réglemente uniquement la localisation à l'aide d'appareils techniques de surveillance tels que les dispositifs employant les systèmes mondiaux de navigation par satellite. En ce qui concerne la recherche à l'aide d'antennes relais, il faut se référer aux dispositions sur la surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)[1381].

1752 La distinction entre les deux méthodes de géolocalisation paraît plus théorique que pratique, puisque l'art. 282 al. 4 CPP renvoie à la procédure de surveillance des télécommunications. Néanmoins, principalement quant au champ d'application, les conditions pour la localisation par GPS et celle par téléphonie mobile ne sont pas identiques[1382].

1753 Les données concernant l'emplacement d'un téléphone mobile sont considérées comme des données accessoires à propos desquelles des renseignements peuvent être obtenus au sens de l'art. 273 CPP[1383]. Le champ d'application de cet article s'étend pour tous les crimes, délits ou contraventions au sens de l'art. 179*septies* CP.

1754 La localisation par GPS est, quant à elle, soumise au respect de l'art. 269 CPP qui limite, à son alinéa 2, l'usage d'une surveillance par satellite à une liste prédéfinie d'infractions.

1755 N'ayant pas voulu reprendre la liste de l'art. 269 al. 2 CPP à l'art. 273 CPP – estimant que l'atteinte aux droits de la personnalité est moins grave lors de la récolte des données de facturations et des données accessoires –, le législateur a créé une différenciation légale entre deux modes de localisation alors même que le résultat fourni, soit le positionnement de l'individu et/ou de l'objet, est identique.

[1380] BSK-StPO-KATZENSTEIN, EUGSTER, art. 280 N 36-37; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 466; STALDER, VERGÈRES, p. 62; StPO-HANSJAKOB, art. 280 N 20-22.

[1381] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 270; StPO-HANSJAKOB, art. 280 N 9.

[1382] MÉTILLE, Thèse, p. 175.

[1383] CR-CPP-BACHER, ZUFFEREY, art. 273 N 4; SCHMID, Praxiskommentar, art. 273 N 2; StPO-HANSJAKOB, art. 273 N 2.

1756 Avant l'entrée en vigueur du CPP, la localisation par GPS nécessitait une base légale pour être applicable, alors que le positionnement à l'aide d'un appareil de téléphonie mobile existait déjà dans la LSCPT et l'OSCPT. La volonté du législateur de conserver les normes préexistantes en ne les modifiant que légèrement a créé cette distinction entre les deux méthodes de localisation qui, à notre sens, ne se justifie guère.

1757 Nonobstant les considérants historiques sur l'existence d'une norme légale préalablement à l'édiction du CPP, il eut été préférable, pour assurer la sécurité juridique, de prévoir une unique réglementation lorsque les appareils GPS ou de téléphonie mobile sont employés pour localiser une personne ou un objet.

1758 Relevons encore que, s'il s'agit de localiser le téléphone mobile grâce au module GPS intégré dans l'appareil, le positionnement dépend alors du système satellitaire. La surveillance est donc soumise au régime des art. 280-281 CPP.

b) Le dispositif légal pour la localisation à l'aide d'appareils de téléphonie mobile

1759 Les systèmes de localisation par ondes hertziennes font partie des télécommunications (art. 2 al. 1 let. a OIT).

1. Le positionnement d'un téléphone mobile déterminé

1760 Pour obtenir les données de positionnement, le recours au fournisseur du service de télécommunication est nécessaire (art. 15 al. 1 à 5 LSCPT et art. 17 al. 3 à 7 OSCPT).

1761 Aux fins de localiser une personne ou un objet, la surveillance des télécommunications peut être ordonnée pour déterminer et transmettre simultanément ou périodiquement l'identification cellulaire (Cell ID), la position et la direction d'émission de l'antenne relais avec laquelle l'appareil de téléphonie mobile est momentanément relié (art. 16 let. b OSCPT *cum* 273 al. 1 CPP pour la surveillance en temps réel). Lorsque la communication n'est pas établie, le fournisseur du service de télécommunication met à disposition et transmet simultanément ou périodiquement l'identification cellulaire, la position et la direction d'émission de l'antenne avec laquelle l'équipement terminal de la personne surveillée est relié au moment de la communication (art. 16 let. c ch. 3 OSCPT *cum* 273 al. 1 CPP). En cas de communication, la transmission rétroactive des informations est également possible (art. 16 let. d ch. 3 OSCPT *cum* 273 al. 1 et 3 CPP).

1762 Suite à la modification de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication entrée en vigueur le 1er janvier 2012, le législateur fait référence à "l'identification cellulaire" (Cell ID). Cette notion renvoie aux normes internationales (ETSI) qui préconisent que l'identificateur réel de la cellule soit fourni sous forme de coordonnées géographique et/ou d'adresse postale[1384]. Ainsi, les données de géopositionnement transmises par les divers fournisseurs de service de télécommunications ont un format prédéfini, ce qui simplifie les recherches subséquentes et ne nécessite pas une transformation ou une traduction de l'information.

1763 Au surplus, la procédure de mise en œuvre, d'exécution, de traitement des données et/ou des découvertes fortuites, de levée et de communication de la surveillance relève des art. 269 ss CPP. Elle est, par conséquent, identique à ce qui prévaut pour la surveillance des télécommunications[1385].

1764 Par conséquent, il n'est pas contestable que des bases légales suffisantes existent aux fins de respecter la prévisibilité légale de la surveillance au moyen de mesures de localisation par l'autorité pénale[1386]. Tempérons ce propos en affirmant une fois encore qu'une législation commune pour la surveillance employant les données satellites et le système d'antennes relais serait plus adéquate à la lumière de la sécurité juridique.

2. La recherche par champ d'antennes

1765 La recherche par champ d'antennes qui s'est développée dans la pratique est concrétisée à l'art. 16 let. e OSCPT.

1766 Avant l'entrée en vigueur de la modification de l'OSCPT, le Tribunal fédéral s'était prononcé sur l'inapplicabilité directe de l'art. 269 ou 273 CPP pour autoriser une telle mesure. En effet, en cas de recherche par champ d'antennes un nombre indéterminé d'appels sont saisis avant d'être ajustés pour individualiser concrètement le ou les suspects potentiels[1387].

1767 Pour éviter que des innocents soient atteints dans leur droit personnel par ce type de surveillance "de masse", des conditions supplémentaires à l'art. 269 et 273 CPP étaient

[1384] CSI-DFJP, Guidelines, p. 53-54; CSI-DFJP SSCPT, p. 4-5.

[1385] Partie II, Chapitre 3, I, A, 2, c.

[1386] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 60-63; CourEDH, Affaire *Shimovolos c. Russie*, arrêt du 21 juin 2011, 30194/09, § 68.

[1387] ATF 137 IV 340, 348-349 = JdT 2012 IV 165, 172-173; HANSJAKOB, Antennensuchläufen, n° 10-11 et 13.

exigées par le Tribunal fédéral[1388]. Outre qu'il devait exister une forte suspicion qu'un crime – ou en tout cas une infraction au sens de l'art. 269 al. 1 let. a et b *cum* 269 al. 2 CPP – ait été commis afin de respecter le principe de proportionnalité, ceci excluant donc la surveillance purement préventive et la surveillance répressive des délits ou contraventions[1389], que la personne recherchée devait être individualisable même si elle restait inconnue, et que la mesure devait être employée subsidiairement à d'autres moyens, il fallait encore que le contenu des appels ou des SMS ne soit pas connu – écouté ou lu –, que la collecte et l'analyse se ciblent sur des données anonymes – données de facturation –, et que la regroupement d'informations avec les données de facturation non-anonymisées devait se limiter à un cercle restreint de potentiels suspects. Pour l'accomplissement de cette dernière condition, le quadrillage du réseau devait s'effectuer uniquement lorsque la communication avait été émise dans un lieu connu et à un moment ou durant un laps de temps déterminé[1390].

1768 En respectant ces conditions, le Tribunal fédéral avait relevé que le quadrillage par champ d'antennes n'était pas d'emblée exclu par l'art. 273 CPP, mais que cet article ne constituait pas, à lui seul et en l'état, une norme adéquate[1391].

1769 Pour limiter la controverse et au vu de l'application fréquente de cette surveillance en pratique, le législateur a réglementé – en partie – cette jurisprudence en édictant l'art. 16 let. e OSCPT. Aujourd'hui, il est clairement établi qu'il est possible de recueillir rétroactivement les données relatives au trafic de la totalité des communications par téléphonie mobile à partir du moment où elles ont eu lieu dans un laps de temps déterminé et dans une cellule déterminée[1392].

1770 A noter que, contrairement à la recommandation du Tribunal fédéral, ce n'est pas le catalogue exhaustif de l'art. 269 al. 2 CPP qui est applicable. Ainsi, en cas de crime, délit ou contravention au sens de l'art. 179*septies* CPP, le ministère public peut – moyennant le respect des autres conditions, notamment l'art. 269 al. 1 let. b et c CPP – ordonner une recherche par champ d'antennes.

[1388] ATF 137 IV 340, 349-350 = JdT 2012 IV 165, 173-174.

[1389] HANSJAKOB, Antennensuchläufen, n° 16-17.

[1390] ATF 137 IV 340, 351-352 = JdT 2012 IV 165, 176.

[1391] ATF 137 IV 340, 347-348 = JdT 2012 IV 165, 171-172.

[1392] CSI-DFJP SSCPT, p. 5.

iii. La mise sous surveillance au moyen des systèmes de navigation par satellite ou d'antennes relais par les particuliers

1771 Concernant l'utilisation du matériel de localisation par des personnes privées – nous pensons ici principalement aux balises GPS ou aux balises fonctionnant à l'aide d'ondes radios qui sont à la portée de tous –, ce type de surveillance n'est réglementé ni par le CPP ni par le droit policier.

1772 Les privés sont donc libres d'agir sous couvert du respect de la sphère privée protégée par le Code pénal[1393].

b. Le but et la nécessité de l'ingérence

1773 De l'avis de la Cour européenne, il est indiscutable que la mesure de surveillance par GPS ou – par analogie – par téléphonie mobile répond à des buts légitimes. Dans l'intérêt de la sécurité publique, de la sûreté, de la répression des infractions et de la bonne administration de la justice, ces dispositifs techniques sont des moyens d'investigation et de preuve adéquats[1394].

1774 En outre, la nécessité de l'ingérence implique qu'elle doit correspondre à un besoin de l'Etat et qu'elle soit proportionnée au but poursuivi.

1775 La Cour européenne[1395] et le Tribunal fédéral[1396] ont relevé que, concernant la surveillance par GPS, la subsidiarité de la mesure, sa limitation dans le temps et son application dans le cadre d'une enquête pour des infractions graves étaient des critères permettant de déterminer si la proportionnalité était ou non donnée.

1776 Le Code de procédure pénale aux art. 269-279 et aux art. 280-281 CPP concrétise les critères jurisprudentiels[1397].

1777 Ainsi, le ministère public peut ordonner la mesure de localisation par GPS si des soupçons laissent présumer qu'une infraction prévue à l'art. 269 al. 2 CPP a été commise, que la

[1393] Supra Partie II, Chapitre 3, I, A, 2, d, n° 1232-1233; Supra Partie II, Chapitre 3, I, B, 2, c, i, n° 1451 et 1511-1512.

[1394] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 77.

[1395] CourEDH, Affaire *Uzun c. Allemagne*, arrêt du 2 septembre 2010, 35623/05, § 78-80.

[1396] TF 1P_51/2007 du 24 septembre 2007, c. 3.5.2-3.6.

[1397] Supra Partie II, Chapitre 3, I, A, 2, c, n° 1140 ss; Supra Partie II, Chapitre 3, I, B, 2, c, ii, c), n° 1534 ss.

gravité de l'infraction justifie la mesure et qu'une autre mesure moins invasive n'a pas été concluante ou ne le serait pas. Pour la surveillance de la localisation par téléphonie mobile ou de recherche par champ d'antennes, l'art. 273 CPP est moins strict, mais il limite la mise en œuvre aux crimes, délits et à certaines contraventions, selon la gravité de l'infraction, et à la subsidiarité de la mesure.

1778 En outre, seul un cadre restreint de personnes sont concernées, l'art. 281 al. 1 et 2 CPP ne prévoit l'emploi du dispositif technique GPS qu'à l'encontre du prévenu et des locaux ou des véhicules de tiers si le prévenu se trouve dans les lieux dont le tiers est propriétaire ou utilise les véhicules de ce dernier. L'art. 273 CPP restreint l'objet de la localisation GSM au prévenu et aux tiers si le prévenu emploie le raccordement téléphonique de celui-ci ou si le tiers concerné reçoit des communications pour le compte du prévenu ou émanant de ce dernier. Dans le domaine de la localisation, nous ne voyons que peu d'intérêt à ce que le ministère public ordonne une surveillance pour positionner le téléphone mobile d'un tiers qui reçoit les communications du prévenu ou pour ce dernier. A notre sens, le but légitime – extensivement la nécessité – n'est pas donné par la localisation d'un tiers à moins que des éléments concrets laissent penser que le prévenu est en présence de ce tiers, étant précisé que la solution la plus adaptée reste l'application par analogie de l'art. 281 al. 1 et 2 CPP lorsqu'une surveillance vise à positionner un téléphone mobile[1398].

1779 Quant à la durée, elle est limitée à trois mois renouvelable pour la surveillance en temps réel et la prolongation de la mesure n'est octroyée qu'en cas de nécessité. La surveillance rétroactive est – généralement – limitée, quant à elle, à une période de six mois.

1780 Au vue de ces constatations, la mesure de surveillance par GPS ou de localisation par la téléphonie mobile répondent à un but légitime et la proportionnalité au sens large n'est pas d'emblée exclue.

D. Les données de localisation comme moyen de preuve

1781 Le but de la surveillance par localisation est similaire à ce qui prévaut pour les autres mesures de surveillance[1399]. Avant tout, il s'agit de récolter des informations afin de pouvoir confondre le prévenu grâce à un appareil GPS ou de téléphonie mobile[1400]. Les autorités

[1398] Supra Partie II, Chapitre 3, II, C, 2, a, ii, b), 1, n° 1777 ss.

[1399] Supra Partie II, Chapitre 3, I, A, 3, n° 1235 ss; Supra Partie II, Chapitre 3, I, B, 3, b, n° 1579 ss.

[1400] CARTIER, p. 219; JORNS, ZHENDONG, p. 33.

pénales peuvent ainsi *a priori*[1401] déterminer en permanence si une personne surveillée est présente à un moment donné dans un lieu donné.

1782 Corrélativement aux autres moyens de preuves intrusifs, l'utilisation des informations recueillies à l'aide de la géolocalisation profite aux autorités pénales. Cependant, une multitude d'informations sont fournies par les appareils de localisation complexifiant la tâche d'enquête pour déterminer quelles sont les données utiles et nécessaires pour l'affaire en cause. Il est donc essentiel de cibler au mieux quels sont les jours et/ou lieux concernés par l'information de géopositionnement concernant un individu déterminé, étant relevé que la comparaison avec l'activité délictuelle enregistrée par la police ou le ministère public et les autres éléments de l'enquête limite au maximum les informations de positionnement non-pertinentes.

E. La discussion sur la preuve liée aux moyens de localisation

1783 L'utilisation des données de localisation des appareils GPS ou GSM offre sans conteste un moyen de preuve aux autorités pénales aux fins de démontrer le positionnement d'un individu. N'étant pas une preuve infaillible, les qualités et faiblesses des résultats issus de la localisation doivent être quantifiées et prises en considération afin de déterminer de manière correcte la force probante de ces méthodes techniques.

1. Le potentiel des preuves issues des systèmes de localisation

a. La nature technique de la preuve et son administration à charge ou à décharge

1784 L'avantage de la technicité d'une preuve et ses possibilités d'être administrée à charge ou à décharge ont déjà fait l'objet d'une discussion lors de l'analyse des preuves scientifiques ou des autres preuves techniques[1402]. Nous ne revenons donc que brièvement sur ces deux qualités.

[1401] Infra Partie II, Chapitre 3, II, E, n° 1782 ss.

[1402] Supra Partie II, Chapitre 2, I, C, 1, a, iii, n° 650 ss; Supra Partie II, Chapitre 3, I, A, 4, a, i, n° 1258; Supra Partie II, Chapitre 3, I, B, 4, a, i et ii, n° 1586 et 1592.

i. Les données mathématiques

1785 Les résultats obtenus à l'aide des systèmes de navigation par satellite ou des réseaux de téléphonie mobile sont d'ordre technique. A l'aide des angles d'émission des antennes, du calcul temps-distance entre l'envoi et la réception d'un signal, ou encore du calcul des intersections entre trois antennes relais, soit à l'aide des mathématiques, il est possible de fournir des coordonnées géographiques.

1786 Exception faite des données erronées suite à un problème technique[1403], la véracité du positionnement et son objectivité offrent une valeur probatoire accrue.

1787 En effet, contrairement aux preuves testimoniales, l'autorité pénale bénéficie d'une représentation matérielle des faits qui peut être facilement démontrée directement par quelques formules mathématiques.

ii. Une preuve à charge ou à décharge

1788 Comme tout moyen probatoire, la géolocalisation aide le juge dans la formation de son intime conviction.

1789 Les données de localisation fournissant des informations – quant au lieu et au moment déterminés – sur le positionnement d'une personne ou, tout du moins, sur la présence de son véhicule ou de son téléphone mobile en un lieu, elles servent à la justice pour démontrer la présence d'un individu sur ou près d'une scène de crime, ou au contraire son absence.

1790 Ainsi soit la thèse de l'accusation, soit celle de la défense sont soutenues par les données de positionnement. Le juge peut alors mathématiquement identifier la présence ou non de l'accusé.

b. La connaissance des données de positionnement

1791 Les progrès technologiques ont permis de communiquer, de filmer et d'enregistrer du son ou des images. Cette avancée technologique a offert aux autorités pénales des moyens pour écouter et observer des individus à distance. De façon similaire, les appareils GPS, les téléphones mobiles, le réseau d'antennes relais et l'intégration d'un module GPS dans les

[1403] Infra Partie II, Chapitre 3, II, E, 2, c, n° 1850 ss.

Smartphone se sont démocratisés auprès des particuliers pour leur permettre de se localiser ou de déterminer leur itinéraire. Les autorités pénales ont vu – à juste titre – en ces possibilités l'opportunité de suivre et de localiser les individus.

1792 L'usage le plus commun du géopositionnement permet de répondre aux questions quand, où et éventuellement, lorsque des regroupements sont effectués, avec qui se situait l'individu surveillé[1404], plus exactement l'appareil GPS ou GSM. Ainsi, ce que les techniques de géopositionnement ont offert en transportabilité des individus, la justice l'a utilisé en traçabilité.

1793 En couplant le résultat de la localisation avec les autres informations obtenues en cours d'enquête, il est alors possible de déterminer la présence ou non de la personne surveillée ou, en cas de suspicion de participation à l'acte délictuel, des personnes surveillées avec plus ou moins de certitude[1405]. Lors des surveillances en temps réel, le fait de déterminer la position d'un utilisateur ou d'un individu surveillé peut également permettre son interpellation, éventuellement en flagrant délit.

1794 En outre, le géopositionnement ne sert pas uniquement à fournir une coordonnée spatiale précise à un moment donné. Généralement, l'individu muni d'un GPS, d'un téléphone mobile, ou encore celui qui est surveillé à l'aide d'un appareil exploitant la navigation satellitaire ou les antennes relais se déplace. Il est donc possible d'obtenir plusieurs coordonnées en fonction de la temporalité.

1795 Au fur et à mesure des déplacements de la personne surveillée, des nouvelles données de positionnement sont alors collectées. Leur regroupement permet de reconstituer *a posteriori* les trajets empruntés par le véhicule ou l'objet mobile[1406].

1796 L'autorité pénale peut, avec une relative précision, déterminer le parcours d'une personne suspectée ou d'un prévenu. Cette possibilité peut avoir de nombreux avantages, notamment pour infirmer ou affirmer les dires d'un suspect ou d'un prévenu concernant, par exemple, sa présence à son domicile durant un certain laps de temps.

[1404] HANSJAKOB, Antennensuchläufen, n° 4.

[1405] Infra Partie II, Chapitre 3, II, E, 2, n° 1818 ss.

[1406] CORNU, p. 248; JORNS, ZHENDONG, p. 31.

c. Les autres possibilités offertes à l'aide des données de positionnement

1797 Les systèmes de navigation par satellite ou par ondes hertziennes ne se limitent pas à fournir les données de positionnement. Divers autres usages par l'autorité pénale sont possibles.

i. L'utilité du géopositionnement pour l'exécution des peines

1798 Nous l'avons énoncé à diverses reprises[1407], le géopositionnement offre l'opportunité aux autorités pénales de connaître la localisation d'un individu à un moment précis. Cette technologie peut se coupler avec un système automatisé.

1799 L'utilisation du système GPS avec automatisation complète des informations reçues permet une surveillance complète par géolocalisation. Lorsqu'un appareil GPS est positionné sur un individu, il est alors possible de le suivre personnellement.

1800 Par exemple, le système de bracelets électroniques permettant de surveiller certaines catégories de personnes sous contrôle pénal peut employer le géopositionnement automatisé. Au moyen du bracelet-GPS, d'un récepteur à domicile ou des satellites dans les cas où l'individu se trouvent en dehors de chez lui et d'un ordinateur central, il est possible de déterminer le positionnememnt du prévenu[1408].

1801 Il sied de relever que le bracelet électronique n'emploit pas forcément la localisation à proprement parler[1409]. Certains modèles se limitent à permettre de surveiller une assignation à résidence, soit l'obligation faite au prévenu de reste à son domicile[1410], une limitaton de perimètre, d'exclusion ou d'inclusion selon que la personne soumise à la mesure est interdite d'entrer dans un perimètre ou de sortir d'une zone prédéfinie[1411], ou encore la surveillance électronique qui offre la possibilité de surveiller le prévenu dans tous ses déplacements et ne le laissent libre dans ses mouvements[1412]. Les deux derniers modes de procéder emploient la technologie GPS, ce recours n'est pas obligatoire pour la première technique[1413].

[1407] Supra Partie II, Chapitre 3, II, B, 1, n° 1689 ss; Supra Partie II, Chapitre 3, II, B, 2, n° 1704 ss; Supra Partie II, Chapitre 3, II, C, 2, b, n° 1773 ss.

[1408] FERREIRA BOQUET, p. 34.

[1409] Infra Partie II, Chapitre 3, II, B, 3, n° 1861 ss.

[1410] FERREIRA BOQUET, p. 21.

[1411] FERREIRA BOQUET, p. 23.

[1412] FERREIRA BOQUET, p. 24.

[1413] FERREIRA BOQUET, p. 21-24.

1802 L'automatisation a non seulement l'avantage de permettre l'enregistrement et le stockage des données de positionnement afin d'être administrées comme preuve, mais permet également de détecter automatiquement si le trajet suivi par l'individu surveillé n'est pas autorisé ou s'il dépasse les limites géographiques qui lui ont été fixées[1414].

1803 Grâce à cette méthode, l'autorité pénale peut s'assurer du lieu où se trouve la personne surveillée, intervenir en cas de violation des obligations qui lui sont imposées et prévenir la commission d'une possible infraction. Etant un mode de surveillance dans le cadre d'une exécution de peine, le CPP n'est pas applicable. Les dispositions idoines sont de droit cantonal[1415]. En revanche, en cas d'utilisation de cette technologie comme mesure de substitution, l'art. 237 CPP est applicable si une assignation à résidence ou une limitation de périmètre est ordonnée au préalable[1416].

ii. Une aide à l'enquête

1804 La nature technique des méthodes de localisation offre un dispositif facilitant grandement les tâches d'enquête.

1805 Contrairement à la filature (art. 282 ss CPP) qui demande du temps, de la stratégie et des moyens en personnel importants. La géolocalisation est simple, rapide et ne mobilise que peu de personnes durant un laps de temps restreint.

1806 La technicité de la localisation GPS ou par téléphonie mobile – jointe éventuellement avec l'automatisation complète – permet par conséquent d'économiser du temps d'enquête et de limiter les ressources nécessaires, sans compter qu'elle offre également un moyen probatoire matériel contrairement à l'observation qui relève des informations perçues et indiquées par un ou des agents de police.

iii. Le système des boîtes noires ou ISA et le projet Via sicura

1807 Concernant les systèmes de navigation par satellite, les appareils GPS peuvent être couplés à d'autres techniques afin de récolter des données ne se limitant pas au pur positionnement,

---

[1414] BERLOVAN, n° 16-18; HANSJAKOB, forumpoenale 2011, p. 302; LEMAN-LANGLOIS, BRODEUR, p. 76 ; StPO-HUG, SCHEIDEGGER, art. 237 N 10.

[1415] FERREIRA BOQUET, p. 65 ss.

[1416] FERREIRA BOQUET, p. 122-125.

ou d'actionner un autre appareil ou logiciel. Nous faisons ici référence au système ISA – Intelligent Speed Adaptation – auquel fait référence le projet "Via sicura" de l'OFROU.

1808 En premier lieu, les boîtes noires utilisées depuis quelques années par les assureurs permettent d'obtenir un certain nombre d'informations. Ainsi, en consultant les données directement ou à distance, et en temps réel, en cas d'accident ou en cas de divers événements prédéfinis, les assureurs peuvent obtenir des informations sur le type de conduite, la vitesse, la durée du freinage de leur client ou encore la distance annuelle parcourue[1417].

1809 En deuxième lieu, le système ISA surveille en permanence la vitesse du véhicule équipé. Initialement, la technicité du système ISA offrait un appui au conducteur et non pas à l'autorité pénale.

1810 Cependant, le recensement des tronçons de route avec la vitesse maximale imposée, l'enregistrement de la position d'un véhicule et la surveillance de la vitesse dudit véhicule peuvent être utiles pour constater et/ou prouver la commission d'une infraction. Ces données peuvent également servir à surveiller un conducteur ou être employées à titre purement préventif notamment en cas de risque de récidive chez un chauffard.

1811 Le projet Via sicura se sert d'ailleurs des avantages du système ISA afin de prévenir ou prouver matériellement des infractions aux règles de la circulation routière[1418].

iv. La recherche par champ d'antennes

1812 Concernant les systèmes de localisation par ondes hertziennes, l'autorité pénale peut recourir à la recherche par champ d'antennes afin d'obtenir des informations pour l'investigation.

1813 En analysant les données spécifiques d'une antenne, il est possible d'obtenir des informations importantes.

1814 Le premier cas qui peut venir à l'esprit est l'identification d'un suspect inconnu[1419]. Lorsqu'un appel est émis à un moment et dans un lieu déterminé, les recherches quant aux données issues de l'antenne relais considérée fournissent un ou des numéros de téléphone, extensivement il est possible d'identifier le titulaire du raccordement et d'enquêter en

[1417] GARSTKA, p. 90-91; GRIMM, p. 95; VOGGENAUER-VON BOTHMER, p. 103.

[1418] RÜFENACHT, p. 4. Supra Partie II, Chapitre 3, II, B, 1, b, n° 1694 ss.

[1419] HANSJAKOB, Antennensuchläufen, n° 5.

fonction. Au vu du trafic important des communications mobiles, il est préférable de connaître l'information relative au moment d'émission à la seconde près d'où est passé l'appel afin de cibler au mieux le numéro concerné et de limiter le plus possible les atteintes aux libertés personnelles.

1815 Dans un second cas, la recherche par champ d'antennes peut être effectuée à l'aveugle. Par exemple, l'autorité pénale constate l'exécution d'un même mode opératoire sur plusieurs scènes de crime. Le quadrillage du réseau et le regroupement des données identiques des diverses antennes relais de la zone où les crimes ont été commis peuvent permettre l'identification d'un suspect ou de participants multiples[1420].

1816 Ces possibilités offertes par la technique du balayage d'antennes ne doivent pas être utilisées de manière abusive par l'autorité pénale. L'utilisation systématique et générale de ces moyens de localisation serait considérée comme du *fishing expedition* et partant, serait contraire au droit.

1817 Par conséquent, il est essentiel que la recherche par champ d'antennes respecte les conditions légales, que le moment et le lieu soient suffisamment déterminés ou que la réitération du mode opératoire soit avérée.

1818 A notre avis, pour respecter le principe de proportionnalité, il est préférable de limiter la recherche à un laps de temps précis de quelques minutes au plus lorsqu'il s'agit d'établir l'identité du titulaire d'un raccordement. Pour les mêmes raisons, il est essentiel qu'en cas de recherche à l'aveugle, le fournisseur du service de télécommunication ne transmette que les données préalablement confrontées et qui sont identiques sans laisser le soin à l'autorité pénale de trier les informations.

2. Les faiblesses et problématiques des preuves issues des systèmes GPS et GSM

a. L'interprétation nécessaire des résultats de positionnement

1819 Les méthodes de localisation automatisée visent à réduire le nombre de contrôles sur le terrain et des ressources nécessaires aux filatures. Néanmoins, il ne faut pas en déduire que les résultats obtenus sont clairs, précis et ne nécessitent aucune interprétation ou que le travail d'enquête est inutile.

[1420] HANSJAKOB, Antennensuchläufen, n° 5.

1820 La localisation d'un individu au moyen des systèmes GPS ou GSM ne permet pas de confondre formellement le suspect, ni d'exclure sa culpabilité.

i. En cas de correspondance positive

1821 Une correspondance positive n'indique pas nécessairement que le suspect ou l'accusé était présent au moment de l'infraction, mais uniquement que son véhicule muni d'un GPS, qu'un autre appareil de navigation par satellite ou que son téléphone mobile était à proximité de la scène de crime[1421].

1822 Il n'est d'emblée pas exclu que le propriétaire du véhicule ou de l'objet permettant d'obtenir les données de positionnement ne soit pas à proximité de son bien. Il peut en effet avoir prêté sa voiture ou son téléphone, avoir été victime d'un vol ou d'un emprunt non autorisé, ou avoir perdu son appareil mobile.

1823 En outre, dans l'hypothèse où il est possible de déterminer la présence sur les lieux du propriétaire du bien, de son emprunteur ou du voleur, il n'est pas impossible que l'auteur de l'infraction soit un tiers présent au même lieu et au même moment sans qu'il soit lié à la personne surveillée.

ii. En cas de correspondance négative

1824 Une correspondance négative ne signifie pas que le propriétaire de l'appareil GPS, du véhicule ou du téléphone mobile ne se trouvait pas sur les lieux d'une infraction.

1825 Il existe parfois des "faux-négatifs". Le suspect ou l'accusé a effectivement commis un acte délictuel sans que le lien géographique ne soit mis en évidence à l'aide des systèmes de localisation simplement parce que le téléphone portable ou le véhicule munis d'un appareillage GPS n'a pas été utilisé, qu'il était hors-zone de couverture, etc.

1826 En outre, lorsque l'appareil GPS localisé est celui d'une voiture, l'autorité pénale doit encore prendre en considération les déplacements entre ledit véhicule et la scène de crime. Le choix de la distance va dépendre étroitement du trajet que l'auteur va réaliser pour commettre son infraction.

[1421] BIRRER, TERRETTAZ-ZUFFEREY, p. 498; CARTIER, p. 222; CORNU, p. 246 et 248.

1827 Dans l'hypothèse où le véhicule est utilisé pour réaliser l'acte délictuel, la distance avec la scène de crime n'a pas lieu d'être considérée.

1828 En revanche, si l'auteur-récidiviste a pour habitude d'effectuer un trajet à pied d'une certaine longueur pour être plus difficilement repéré, la prise en compte d'une distance de quelques kilomètres – maximum 5 kilomètres – n'est pas déraisonnable.

1829 Ce dernier exemple peut être appliqué par analogie quant à la réception du signal émis par un téléphone mobile. Il n'est pas exclu que l'auteur se serve de son portable – par exemple, pour organiser une livraison de stupéfiant – et se déplace sur les lieux de l'infraction sans être muni dudit téléphone ce qui empêche de le localiser. Une distance également de quelques kilomètres peut être prise en compte pour considérer les trajets de l'auteur sans quoi les risques d'obtenir un faux positif sont accrus.

iii. Le travail d'enquête

1830 Les données de positionnement n'étant pas suffisantes par elles-mêmes, il ne s'agit que d'un indice. Pour s'assurer de ce qu'elles démontrent réellement, la localisation doit faire l'objet d'une enquête approfondie et être intégrée dans un faisceau de preuves.

1831 La géolocalisation permet uniquement de cibler les vérifications usuelles d'enquête sur un ou plusieurs individus. La phase d'enquête ne se résume donc pas à une simple formalité. Lorsqu'une coordonnée géographique est fournie aux autorités pénales, une procédure complémentaire doit être réalisée.

1832 La première étape s'effectue par comparaison. L'utilité d'une donnée de positionnement en procédure pénale n'existe que si elle est couplée avec une infraction. Il est donc nécessaire de vérifier que la position géographique et le moment du signal soient similaires au lieu et au moment du déroulement de l'acte délictuel.

1833 La deuxième étape est l'examen des informations obtenues. Si une corrélation entre les données de positionnement et la scène de crime a pu être déterminée, l'autorité pénale doit se demander qui était l'utilisateur du véhicule, du téléphone mobile ou de tout autre appareil GPS ou GSM. Une fois déterminé, il faut encore vérifier que la personne identifiée n'avait pas une raison particulière de se trouver dans la zone à proximité de l'infraction[1422].

[1422] BIRRER, TERRETTAZ-ZUFFEREY, p. 498.

1834 La troisième étape est le couplement entre les informations issues de la localisation et les autres moyens de preuves alléguant les faits reprochés. Ce n'est que dans l'hypothèse où un faisceau de preuves existe que la donnée de positionnement trouve son intérêt en justice.

1835 En tant que telle, prise isolément, la donnée de positionnement démontre uniquement qu'un objet mobile, soit déplaçable avec facilité, s'est trouvé à proximité du lieu de commission d'un acte délictuel. Une simple coordonnée géographique ne démontre donc que peu – voire pas – d'éléments de fait concrets de l'affaire. Par conséquent, seule, elle n'a quasiment pas de valeur probatoire.

1836 Même une localisation en temps réel a sa marge d'interprétation. En effet, elle permet de lier avec certitude un individu et un lieu, mais l'identification formelle de cette personne comme auteur d'une infraction n'est pas prouvée. Il est donc également nécessaire de recourir à d'autres moyens probatoires.

b. L'approximation de la localisation

1837 L'exploitation des données de positionnement ne s'avère utile à l'autorité pénale que si elles sont de qualité ou, tout du moins, s'il est possible de quantifier l'approximation, voire le risque d'erreur. A cette fin, il faut distinguer la qualité des données en fonction de la méthode de localisation employée.

i. Les données issues des systèmes de navigation par satellite

1838 Le principe du GPS se base sur la multilatération, soit la réception du signal émis par trois satellites afin de définir une coordonnée en deux dimensions à l'aide des données temps et distances du signal émis. Une erreur dans une information nécessaire au calcul des coordonnées faussent par conséquent la localisation du récepteur GPS. Les principaux écarts de positionnement tiennent au retard des signaux dans leur déplacement, à la précision des horloges des satellites, aux perturbations extérieures et aux obstacles réfléchissants[1423]. Des corrections peuvent être apportées pour réduire ces erreurs: modèles de l'ionosphère, conception spéciale des signaux, etc. En outre, il est toujours possible de quantifier l'approximation du positionnement et d'effectuer manuellement un correctif.

[1423] DODEL, HÄUPLER, p. 83-86 et 118-123; OOSTERLINK, p. 89.

1839 Généralement, la précision d'une localisation à l'aide d'un récepteur GPS est d'environ 10 mètres[1424]. Pour les besoins d'une recherche, cette approximation n'est pas problématique. En revanche, dans le cadre d'une poursuite pénale, une différence même de quelques mètres peut servir ou desservir la thèse de l'accusation ou de la défense.

1840 Prenons deux exemples, l'un est un crime commis en pleine nuit dans une zone rurale où n'est sise aucune maison, bâtisse ou tout autre bâtiment justifiant la présence d'un individu en ces lieux qui ne promènerait pas son chien et n'est pas un passionné des animaux diurnes; l'autre est un crime commis au centre-ville en pleine nuit à l'angle de deux rues à proximité de l'allée n°10 faisant partie d'un bloc de bâtiment.

1841 Dans le premier cas, la zone isolée ne laisse que peu de doute sur la présence du véhicule ou d'un autre appareil GPS du suspect ou de l'accusé. Couplé avec les autres éléments de l'enquête, la présence de l'individu est alors difficilement explicable. La différence possible de plus ou moins 10 mètres est pratiquement insignifiante et influe peu, voire pas, sur la qualité et la valeur probante de la localisation.

1842 Dans le deuxième cas, d'après les données de positionnement, le véhicule du suspect s'arrête un court instant devant l'allée n° 10. En réalité, le suspect ou le prévenu maintient qu'il n'était pas sur la rue A où est sise l'entrée de l'allée mais sur la rue B devant une autre allée sise à 10 mètres en diagonale de l'allée n° 10. Il n'a en outre pas vu quoique ce soit, puisqu'il était parqué un court instant sur une rue perpendiculaire à celle où le crime a eu lieu. Dans cette hypothèse, les 10 mètres d'approximation jouent un rôle fondamental. Un mauvais concours de circonstances est possible ce qui laisse un doute sur la qualité du positionnement.

1843 L'exemplification n'a pas pour but de nier toutes qualités aux données de localisation. Des mesures extrêmement précises ne peuvent être réalisées qu'en intégrant les éléments locaux pouvant créer l'approximation dans l'interprétation du géopositionnement. Dans le cas où les risques d'erreurs ne sont pas pris en considération, selon le contexte et la zone géographique, un travail d'enquête, d'interprétation et de création d'un faisceau de preuves sont déterminants pour juger de la réelle valeur probante de la preuve par GPS.

[1424] ANDREANI, p. 16; BIRRER, TERRETTAZ-ZUFFEREY, p. 485-486.

ii. Les données issues des systèmes de télécommunication mobile

1844 L'identification de la cellule (Cell ID) utilisée par les autorités suisses manque de précision dès lors qu'elle est étroitement liée à la zone de desserte des antennes de téléphonie. Ainsi, la précision de localisation du téléphone mobile varie selon la taille de la cellule qui dépend de la densité des relais et de leur zone de desserte[1425].

1845 En ville, le nombre d'antennes de téléphonie est plus important limitant la taille des cellules. Dans le milieu urbain, la localisation peut être imprécise d'une centaine de mètres. En campagne, la densité des antennes est moindre, la précision est estimée de 3 kilomètres à 10 kilomètres. A certains endroits isolés, l'erreur de positionnement peut atteindre bien plus de 10 kilomètres[1426]. Majoritairement, 41% de toutes les antennes desservent un territoire d'un kilomètre et 58% s'étendent à 10 kilomètres[1427].

1846 En d'autres termes, plutôt que de parler de la géolocalisation au sens strict, il faut reconnaître que la donnée de positionnement obtenue grâce à la téléphonie mobile n'offre qu'une identification de la zone d'appel à un moment précis[1428].

1847 Pour affiner la localisation, deux possibilités existent selon que la personne surveillée se déplace ou non.

1848 En cas de déplacement, l'activation d'une autre antenne offre la possibilité de coupler les informations, d'isoler une zone de jonction et ainsi de restreindre la zone de déserte.

1849 Dans l'hypothèse où aucun déplacement n'est effectué et pour obtenir une zone plus précise, il n'y a pas d'autre moyen que d'accroître la densité du nombre de relais sur le territoire. Cependant, la mise en fonction d'autres antennes relais ne ferait que de diminuer la taille de la zone de desserte. Il n'en reste pas moins que la donnée de positionnement – même plus précise ou plus exactement limitée à un champ territorial plus restreint – ne fournit que l'emplacement approximatif dans une zone et non pas une localisation précise.

1850 Par conséquent, l'identification Cell ID n'est qu'un moyen de localisation vague qui ne peut assurer de la présence d'un individu, plus précisément de son téléphone mobile, en un lieu

---

[1425] CARTIER, p. 205.

[1426] CARTIER, p. 205; HANSJAKOB, BÜPF/VÜPF, art. 1 N 18; OFCOM, infomailing 2008, p. 8.

[1427] OFCOM, infomailing 2005, p. 13.

[1428] BAUER, FREYNET, p. 65; BIRRER, TERRETTAZ-ZUFFEREY, p. 485; CARTIER, p. 205.

plus ou moins étendu dans l'espace. Il ne s'agit donc pas d'administrer une preuve certaine et irréfragable d'un point géographique déterminé.

c. Les dangers potentiels et les techniques de sécurité

1851 Comme tout moyen technique, il n'est pas exclu qu'un problème survienne lors de l'utilisation de la localisation par satellite ou ondes hertziennes. Il peut s'agir de pannes, de "*bugs*" ou de "*hacking*".

i. Les problèmes techniques fréquents et leurs conséquences

1852 Le cas le plus fréquent est une panne complète, sectorielle ou d'un composant utile à la localisation.

1853 Lorsque la panne est complète et s'étend à une partie considérable du territoire ou du service de géopositionnement, elle est facilement décelable. Sa prise en considération afin d'éviter les erreurs au sein des données de positionnement est en principe garantie.

1854 En revanche, lorsqu'il s'agit d'une panne sectorielle ou qui concerne uniquement un composant du système précis, la reconnaissance de la panne est plus délicate amenant quelques difficultés dans l'interprétation des résultats.

1855 Dans le cadre de la procédure pénale, si un appareil GPS ou un téléphone portable ne transmet plus, la conséquence est uniquement une absence de données de positionnement. En soi, ce type de panne n'occasionne pas de graves atteintes quant à la valeur probante puisque la preuve n'existe pas.

1856 Au contraire, si un appareil GPS ou un téléphone portable fonctionne et permet d'obtenir une donnée de positionnement alors qu'une panne survient ou une maintenance non prévue a lieu, la donnée peut s'avérer incorrecte.

ii. Les pannes survenant sur les systèmes GPS ou de téléphonie mobile

1857 En cas de panne ou de maintenance sur les systèmes de navigation par satellite, il est rare de pouvoir obtenir une information sur l'emplacement d'un appareil GPS. Le problème n'est donc pas conséquent dans ce domaine.

1858 L'impact sur les systèmes de téléphonie mobile est plus important.

1859 Une panne peut impliquer la reprise du signal émis par une antenne relais plus éloignée. Il est donc impératif qu'en cas de panne, l'opérateur la signale à l'autorité pénale. En effet, l'identification Cell ID concerne une certaine cellule, plus précisément celle dont l'antenne reçoit le signal le plus fort. En cas de panne, il n'est pas exclu que le signal n'aurait pas été capté par la même antenne, notamment parce qu'un signal plus fort aurait été émis sur l'antenne en panne, ce qui change la zone de localisation.

1860 De même, en cas de maintenance du système de téléphonie ou des antennes relais – maintenance relativement fréquente –, l'information doit être transmise à l'autorité. En effet, une maintenance occasionne les mêmes conséquences qu'une panne réseau.

1861 En toute hypothèse, il est essentiel que le fournisseur de service explique quelle conséquence la panne ou la maintenance a créé sur la valeur des données de positionnement.

iii. Le piratage des données GPS et/ou GSM

1862 L'évolution des techniques n'offre pas que des moyens de preuves aux autorités pénales, elle fournit également la possibilité de contrer l'utilisation de ces moyens. Quelques recherches sur internet suffisent à obtenir des informations pour brouiller un système GPS et GSM, ou pour les pirater.

1863 Un nombre considérable de sites en ligne proposent des brouilleurs qui visent à lutter contre l'espionnage ou la surveillance grâce au blocage des ondes employées pour la transmission GPS ou GSM.

1864 D'autres sites internet expliquent notamment la facilité avec laquelle les hackers peuvent pirater un GPS en lançant un faux signal qui se superpose au vrai pour afficher une position et une référence temporelle erronées.

1865 Toutes ces méthodes influent sur la véracité des données de positionnement.

1866 En outre, dans le cas de la localisation par l'intermédiaire des opérateurs de téléphonie mobile, les informations de positionnement sont stockées dans des bases de données. Leur exactitude dépend donc de la sécurité informatique. En effet, une sécurité inexistante ou trop basse ne met pas en échec les tentatives de hacking, de ce fait elle ne permet pas de certifier l'authenticité des données.

1867 Par conséquent, pour juger de la valeur probatoire des données de positionnement, les risques de piratage des données de positionnement et de hacking doivent être pris en considération.

3. L'émergence des puces RFID

1868 Le système RFID est utilisé depuis plusieurs dizaines d'années, notamment pour gérer les stocks des grands magasins, les prêts de bibliothèque ou pour contrôler les accès à certains bâtiments, aux ordinateurs, et il est également employé comme système antivol[1429].

1869 La démocratisation de cette technologie tient principalement au fait qu'une même puce RFID peut atteindre plusieurs finalités, ce qui évite de devoir recourir à diverses méthodes coûteuses et variées[1430]. Par exemple, au sein des entreprises, une puce RFID peut servir pour se déplacer de bâtiments en bâtiments ou à l'intérieur des locaux, pointer ses heures de travail et encore payer à la cafétéria ou aux automates.

1870 Dans le cadre de notre recherche, l'intérêt principal pour la RFID tient à son faible coût et à la miniaturisation de la puce. En effet, la puce RFID devient à ce point minuscule qu'elle peut être intégrée pour marquer de petits objets ou des êtres vivants[1431]. Avec pour conséquence, la possibilité de tracer les porteurs d'une puce.

1871 En tant que technologie se perfectionnant rapidement, nous nous intéressons à son potentiel de localisation. Afin de mieux le cerner, la présente analyse se concentre sur la technologie RFID et ses possibilités d'utilisation par les autorités pénales.

a. Le système d'identification par radiofréquence (RFID)

i. La technologie RFID

1872 Dans sa forme la plus simple, le système d'identification par radiofréquence – RFID – se compose de radio-étiquettes, telles que des étiquettes adhésives ou des puces électroniques, qui sont des marqueurs passifs, et d'un lecteur[1432].

[1429] ARIOLI, THALMANN, p. 550; CNIG, p. 1; MÉTILLE, Thèse, p. 63.

[1430] MÉTILLE, Thèse, p. 63.

[1431] ARIOLI, THALMANN, p. 550; CNIG, p. 1.

[1432] ARIOLI, THALMANN, p. 550; CNIG, p. 1; FERREIRA BOQUET, p. 28; MÉTILLE, Thèse, p. 63.

1873 Les marqueurs ont une petite mémoire qui leur permettent de conserver un identifiant et éventuellement des données complémentaires. Chaque fois qu'un marqueur est à proximité d'un lecteur, celui-ci peut lire les informations et identifier la puce RFID.

ii. Le fonctionnement de la technologie RFID

1874 Pour communiquer, la RFID emploie la radiofréquence. Le lecteur émet des ondes radios à une certaine fréquence pour activer/alimenter les marqueurs afin d'obtenir les informations sises dans la mémoire de la puce RFID[1433].

1875 Comme la communication se base sur la radiofréquence, il n'est pas nécessaire que le marqueur et le lecteur entrent physiquement en contact. La proximité entre l'un et l'autre est suffisante. Ainsi, lorsque les objets marqués par une puce RFID passent près d'un lecteur, ils sont automatiquement détectés même si un grand nombre de puces se succèdent ou sont simultanément proches du lecteur.

1876 Selon le matériel, la fréquence radio utilisée et les sources d'interférences, la portée d'émission des ondes radios et la réception par le marqueur varient. Dans certains cas, la puce RFID doit se trouver à quelques centimètres; dans d'autres, notamment lorsque le marqueur est muni d'une batterie, la distance entre le lecteur et la puce peut être de plusieurs dizaines de mètres[1434].

1877 Généralement, la proximité entre le marqueur et le lecteur doit être relativement proche. Un lecteur d'étiquette intelligente détecte une puce jusqu'à 1 mètre 50[1435]. Néanmoins, il faut admettre que l'évolution de cette technologie va permettre dans un avenir proche de dépasser les quelques dizaines de centimètres nécessaires.

1878 Grâce à la détection, la RFID est donc sans conteste un moyen adéquat pour identifier et de ce fait, localiser un marqueur, extensivement le porteur de la puce[1436]. C'est pourquoi, les autorités d'exécution des sanctions l'utilisent sous la forme d'un bracelet-radiofréquence en cas d'assignation à résidence ou de limitation de périmètre[1437].

[1433] ARIOLI, THALMANN, p. 550; COMMISSION D'ACCES A L'INFORMATION DU QUEBEC, p. 1; CNIG, p. 1; FINKENZELLER, p. 32-42; HODGES, MCFARLANE, p. 62; PFPDT, Rapport 2009/2010, p. 34-36.

[1434] HODGES, MCFARLANE, p. 64 ; MÉTILLE, Thèse, p. 62.

[1435] SCHOBLICK, SCHOBLICK, p. 13-24 et 192-228.

[1436] ARIOLI, THALMANN, p. 551; BONDALLAZ, protection des personnes, p. 415.

[1437] FERREIRA BOQUET, p. 29-30.

iii. Les évolutions et applications récentes de la RFID

1879 A l'appui de l'affirmation voulant que l'évolution technologique permette une communication à une distance considérable, il est suffisant de s'intéresser à trois grandes mises en œuvre de la puce RFID.

1880 En premier lieu, les nouveaux passeports dits électroniques ou biométriques sont composés d'une puce RFID qui contient les données d'identité, soit les informations officielles sur un individu[1438]. Les Etats-Unis sont désireux de développer cette technique afin de pouvoir lire facilement les informations de la puce sans qu'il soit nécessaire d'être proche du marqueur[1439]. Des recherches dans ce sens sont donc entreprises, ce qui au vu des succès technologiques actuels dans divers domaines, notamment informatique, ne devrait pas aboutir à un échec.

1881 En deuxième lieu, des médecins américains implantent sous la peau des patients atteints d'Alzheimer une puce RFID. Ainsi, si le malade disparaît, fuit ou se perd, les recherches sont plus aisées grâce à la RFID et aux données identificatrices mémorisées dans le marqueur[1440]. Il n'est pas exclu que cet usage se développe afin de surveiller des patients atteints d'autres pathologies mentales. D'ailleurs, en Suisse, un projet pilote a été mis en œuvre en 2005 visant à permettre l'identification des personnes munies d'un implant RFID lorsqu'elles se trouvent à proximité d'un lecteur et déterminer la faisabilité de ce système[1441]. Les résultats ne sont pas connus, mais une recherche sur internet démontrent que de plus en plus de pays tente d'intégrer les implants RFID pour identifier des personnes[1442].

1882 En troisième lieu, partant du principe que les dents sont l'organe du corps humain le plus résistant, des chercheurs belges ont implanté une puce RFID dans une dent contenant une sorte de fiche d'identité. En approchant le marqueur du lecteur, il est alors possible de pouvoir lire les informations qui y sont stockées[1443].

[1438] GHERNAOUTI-HÉLIE, p. 108-114; MEIER P., p. 155; MÉTILLE, Thèse, p. 65.

[1439] MEIER P., p. 155; MÉTILLE, Thèse, p. 66.

[1440] Informations disponibles sur le site internet du RFID journal: http://www.rfidjournal.com [consulté le 08.05.2016].

[1441] Nzz, *Chip im Oberarm*, article du 10 avril 2005; Tagesanzeiger, *Funketiketten machen sich an Menschen ran*, article du 6 septembre 2005.

[1442] Informations disponibles sur le site internet Killuminati Suisse: http://www.killuminati.ch/ [consulté le 08.05.2016].

[1443] Emission Nouvo de la RTS, *RFID: la puce fait ses dents*, diffusée le 23 avril 2007.

1883 Concernant cette dernière application de la technologie RFID, vu la faible portée des ondes radios, il faut préciser qu'elle est principalement employée pour identifier un corps méconnaissable. Néanmoins, l'évolution de la technique RFID tendant à miniaturiser le marqueur et également à accroître la distance nécessaire entre le marqueur et le lecteur, il n'est pas exclu que, dans quelques temps, l'introduction d'un marqueur dans une dent puisse servir à tracer des individus.

b. L'exploitation des puces RFID par l'autorité pénale et sa légalité

i. Les types de localisation grâce à la technologie RFID

1884 La technologie RFID peut permettre la localisation passive ou active[1444].

a) La localisation passive

1885 La localisation passive n'est possible généralement que dans des enceintes délimitées comme un bâtiment, un centre commercial, une gare, etc. Eventuellement, ce système peut permettre la surveillance d'un individu astreint à domicile par l'envoi quotidien des historiques du bracelet[1445].

1886 L'objet ou l'être vivant doté d'une puce RFID est détectable dans une zone lors de son passage près d'un dispositif de lecture. Il est alors possible d'identifier un objet ou une personne sise dans l'enceinte délimitée, de les localiser et, en couplant les informations des divers lecteurs présents sur les lieux, de suivre leurs déplacements. Parfois, un récepteur portable peut être employé afin de surveiller, dans un lieu restreint, un prévenu muni d'un émetteur (bracelet électronique, nommé bracelet-radiofréquence)[1446].

1887 Un tel moyen de localisation peut être fort utile pour compléter le positionnement GPS[1447]. En effet, ce dernier n'offre pas la possibilité de détecter la présence d'un individu à l'intérieur d'un bâtiment, alors qu'au contraire, la RFID offre largement cette opportunité lorsque suffisamment de lecteurs sont mis en fonction.

[1444] CNIG, p. 3-4; FERREIRA BOQUET, p. 28.

[1445] FERREIRA BOQUET, p. 29.

[1446] FERREIRA BOQUET, p. 27-28.

[1447] FERREIRA BOQUET, p. 39.

b) La localisation active

1888 La localisation active est possible moyennent le couplement de la puce RFID avec un GPS ou un émetteur radio[1448].

1889 Grâce à cette méthode, la localisation à l'aide de la technique RFID ne se limite plus à une enceinte restreinte, mais s'étend entre 30 à 60 mètres[1449]. Néanmoins, l'usage d'un lecteur, ordinateur central de contrôle par exemple, reste obligatoire pour permettre de réceptionner les signaux émis par le boîtier-radiofréquence qui sont ensuite transmis au moyen du réseau de téléphonie fixe ou mobile[1450].

ii. La légalité en droit suisse de la géolocalisation à l'aide de la RFID

1890 En elles-mêmes, les puces RFID ne contiennent aucune information de géolocalisation. Ce n'est qu'au passage d'un lecteur qu'elles sont détectées, la gestion automatisée de ces lecteurs peut permettre de déterminer où se trouve une puce RFID en fonction de l'emplacement du lecteur.

1891 Entre deux lectures, aucune information de positionnement n'existe. Néanmoins, en fonction de la densité du réseau de lecteur, la RFID peut fournir également un moyen de traçabilité et suivre les déplacements du marqueur, corrélativement au suivi d'un téléphone mobile ou d'un GPS.

1892 Sans conteste, en déposant un marqueur sur un objet, sur le corps d'un individu ou sur ses habits, voire en implantant une puce RFID dans le corps d'un être humain, la technologie RFID sert de moyen de localisation.

1893 Dans le cadre de la procédure pénale, le système RFID peut donc se comparer aux mesures de surveillance.

1894 Dès lors que contrairement à l'identification Cell ID, la RFID n'est pas une donnée accessoire (art. 273 CPP) et que la personne concernée n'est pas sujette ou partie à la communication effectuée *via* les ondes radios, les dispositions sur la surveillance des télécommunications ne sont pas applicables (art. 269-279 CPP)[1451].

[1448] ARIOLI, THALMANN, p. 553; MATTERN, p. 15-18.

[1449] FERREIRA BOQUET, p. 29.

[1450] FERREIRA BOQUET, p. 29.

[1451] BONDALLAZ, protection des personnes, p. 416.

1895 La RFID étant un appareillage technique permettant de localiser un marqueur, il s'agit d'un "dispositif technique de surveillance aux fins de localiser une personne ou une chose" (art. 280 let. c CPP), corrélativement au GPS. La procédure pour employer cette méthode de manière préventive ou répressive est par conséquent identique à celle prévalant pour le géopositionnement par satellite[1452].

1896 Relevons encore qu'en cas d'emploi d'un bracelet-radiofréquence, dans le cadre de l'exécution d'une peine, le CPP n'est pas applicable. Il faut alors se référer aux normes cantonales en la matière[1453]. Par ailleurs, si cette méthode technique est employé à titre de mesures de substitution, l'art. 237 CPP est applicable, avec la précision qu'une assignation à résidence ou une limitation de périmètre doit, au préalable, être prononcée[1454].

c. Les difficultés ou obstacles liés à l'utilisation de la RFID comme moyen de localisation et moyen de preuve

1897 Pour être employée comme preuve, une donnée issue de la localisation par la technologie RFID ne doit pas être manipulée, erronée ou incorrecte.

1898 Comme tout composant informatique, les puces RFID peuvent contenir des virus qui modifient les données communiquées au lecteur[1455], être falsifiées ou contrefaites[1456], et il est également concevable qu'elles soient techniquement manipulées pour modifier les écritures inscrites[1457]. Quant au lecteur, des failles de sécurité ne sont pas non plus exclues.

i. La sécurité du système de fonctionnement RFID

1899 En principe, les informations du marqueur ne sont pas librement accessibles. Une clé d'accès crypte toutes les données contenues dans la puce. Cependant, les systèmes RFID employant pour fonctionner un canal de radiocommunication et des composants informatiques, il existe un certain nombre de conséquences pour la sécurité du fonctionnement.

[1452] Supra Partie II, Chapitre 3, II, C, 2, a, i, n° 1736 ss.

[1453] FERREIRA BOQUET, p. 65 ss.

[1454] FERREIRA BOQUET, p. 122-124 et 247.

[1455] MÉTILLE, Thèse, p. 64.

[1456] SCHOBLICK, SCHOBLICK, p. 146.

[1457] Dailymail, *New ID cards are supposed to be unforgeable*, article du 6 août 2009.

1900 Une expérience effectuée sur la puce RFID d'un passeport hollandais a démontré que le marqueur pouvait être lu à l'aide d'un dispositif bon marché et accessible à la population. La même étude démontre qu'en quatre heures maximum, la clé de cryptage d'un passeport britannique peut être décodée[1458].

1901 Cette expérience confirme que toute transmission peut être détectée par un autre équipement situé à portée, notamment par une interface de lecture pirate ou non-autorisé[1459], puis être décodée. D'autres expériences ont également démontré la fragilité de ce système[1460]. Quiconque désire espionner le système peut donc le faire relativement facilement et de manière secrète. La possibilité de pouvoir déchiffrer la clé de cryptage accentue les risques liés à la communication d'informations à l'aide du lecteur et marqueur RFID. Il n'est alors pas exclu qu'une puce RFID subissant une attaque de type hacking, soit modifiée et/ou copiée.

1902 En outre, une autre conséquence de l'emploi de la radiofréquence, une puce RFID peut être totalement inutilisable. Un autre équipement – comme un brouilleur – est en effet susceptible d'émettre et par conséquent de créer des interférences. Il n'est alors plus possible pour le lecteur de communiquer avec la puce et de lire les informations, extensivement de localiser le bien ou la personne concernée. Par conséquent, la RFID devient inexploitable. Notons qu'il y a peu de chances qu'une interférence liée à l'utilisation de la même fréquence par un autre appareil intervienne, il s'agira donc vraisemblablement d'une utilisation malveillante dans le but de limiter les possibilités de cette technologie.

ii. Les obstacles au succès de la RFID

1903 Pour être pleinement opérationnel et utile à l'autorité pénale, chaque individu ou objet doit être suivi individuellement.

1904 Une surveillance personnelle produit – généralement – un nombre considérable de données. Pour pouvoir être employée avec une pleine efficacité, il faut coupler la technologie RFID avec un système automatisé de gestion de données afin de permettre la mémorisation et le traitement des informations recueillies. Sans un tel système informatique, il semble

[1458] The Guardian, *Cracked it*, article du 17 novembre 2006; MÉTILLE, Thèse, p. 66.

[1459] BONDALLAZ, protection des personnes, p. 418; HODGES, MCFARLANE, p. 64; SCHOBLICK, SCHOBLICK, p. 149.

[1460] Forbes, *Hacker's demo shows how easily credit cards can be read through clothes and wallets*, article du 30 janvier 2012.

fortement probable que le but désiré par la surveillance *via* RFID ne pourrait pas ou difficilement être atteint.

iii. L'emploi comme moyen probatoire des données issues de la technologie RFID

1905 Avec le développement de la technologie RFID, le nombre de données exploitées et enregistrées, les opérations de traitement ne se réalisent plus physiquement, mais à l'aide de systèmes électroniques exposant d'avantage les données à certains comportements délictueux, tels que l'introduction de virus ou le hacking.

1906 La sécurité informatisée du système de fonctionnement RFID est dès lors essentiel pour éviter au maximum les risques liés à des écritures, des lectures ou des interceptions frauduleuses. Sans un minimum de sécurité contre les intrusions, les données issues de l'identification RFID ne peuvent pas être authentifiées et leur véracité n'est pas certaine avec pour conséquence une faible valeur probante.

1907 Dans l'hypothèse où, malgré la mise en œuvre de moyens de sécurité, un cas d'intrusion d'un tiers non-autorisé est détecté ou supposé, le recours à des experts pour déterminer les conséquences sur la force de convictions des données obtenues est nécessaire afin d'éviter au maximum les erreurs d'interprétation.

1908 Au surplus, les avantages et les inconvénients pouvant influer sur la force de démonstration de la preuve RFID sont similaires à ce qui prévaut pour la localisation par GPS ou par téléphonie mobile[1461].

III. Les techniques informatiques et les systèmes de gestion de base de données

1909 Constatant l'utilisation accrue par la population du matériel informatique pour stocker des données, effectuer des recherches et/ou communiquer, les autorités pénales ont vu dans ce moyen technologique une aide et un support à l'enquête. En outre, les opportunités offertes par le stockage des données et l'analyse automatisée ont également retenu l'attention des autorités.

[1461] Supra Partie II, Chapitre 3, II, E, 1 et 2, n° 1783 ss.

1910 Ce domaine technologique est vaste et varié. Une thèse complète pourrait traiter des divers sujets informatiques utiles à la procédure pénale. La présente partie ne se veut donc pas exhaustive. Néanmoins, nous ne pouvons pas traiter des nouvelles technologies sans évoquer les ordinateurs et leurs potentiels.

1911 Nous analysons donc ici uniquement les sujets – actuellement – les plus opérants dans le cadre de la preuve pénale. Les preuves informatisées ou informatiques font l'objet d'une première analyse (A.) et une seconde partie étudie l'informatique comme aide à l'investigation criminelle (B).

A. Les moyens informatiques

1. L'introduction

1912 Avec l'évolution du Peer-to-Peer, du téléchargement illégal, de l'utilisation des réseaux sociaux ou des moyens de communications informatiques et de l'emploi d'ordinateur pour commettre des actes délictuels, l'observation ou l'infiltration d'agent par l'autorité pénale des blogs, forums ou "chat" et les preuves par IP ou adresses MAC, par disques durs, plus particulièrement par fichiers informatiques, ont fait parler d'eux dans le monde judiciaire, notamment suite à la réglementation Hadopi adoptée en France[1462].

1913 L'interception des communications électroniques *via* les services de messageries et les conversations VoIP ont déjà fait l'objet d'une étude approfondie[1463]. C'est pourquoi nous nous intéressons exclusivement à la surveillance sur Internet, plus spécifiquement des forums de discussion, des blogs ou des *chatroom*, à la surveillance de l'adresse IP ou MAC et à la perquisition des documents informatiques.

1914 Plus particulièrement, il s'agit dans cette partie de notre étude de décrire la procédure touchant à la récolte d'informations par ou grâce aux matériels ou fichiers informatiques, et d'exposer l'apport d'une preuve électronique issue de la surveillance sur Internet ou provenant des renseignements de télécommunication.

[1462] Loi française n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Loi HADOPI); Loi française n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (Loi HADOPI 2).

[1463] Supra Partie II, Chapitre 3, I, A, n° 1101 ss.

2. Quelques notions techniques et définitions

a. Le réseau internet et les groupes de discussion

1915 Le réseau Internet est un réseau de télécommunication constitué de divers réseaux employant le protocole TCP/IP[1464]. En tant que réseau public et ouvert à tous ceux qui disposent d'un ordinateur ou d'un autre appareil similaire et d'une connexion Internet, il constitue le principal environnement numérique.

1916 Le développement de l'Internet a offert de nombreux services aux utilisateurs[1465].

1917 La messagerie électronique – nous l'avons vu – permet d'échanger des courriers et des fichiers informatiques entre usagers. Les logiciels de communication, tels que les logiciels VoIP – Skype, TeamSpeak, Gizmo, etc. – ou les services de messageries instantanées – IRC, MSN, ICQ, etc. –, servent également à transmettre des données *via* le réseau Internet. Nous ne revenons pas en détails – dans cette partie de l'étude – sur ces services Internet lorsque les données sont en transite sur le réseau[1466].

1918 Les groupes ou forums de discussion sont des pages internet ou des applications permettant d'échanger des points de vue avec les autres internautes. Certains groupes ou forums sont publics ce qui permet à tout un chacun de lire les informations ou les discussions entre des tiers[1467], voire d'intervenir en tant qu'"invité"; d'autres nécessitent une inscription et une authentification pour participer activement ou passivement à la discussion.

1919 Le *World Wide Web*, appelé communément le "web" ou familièrement "internet" – à ne pas confondre avec "Internet" qui correspond aux réseaux interconnectés –, permet, à l'aide d'un navigateur, d'obtenir toute une série d'informations sur une quantité infinie de domaines. Il est ainsi possible d'apprendre facilement en quelques clics de souris: comment réaliser une bombe, pirater un réseau Internet ou un ordinateur, se procurer illégalement une arme, falsifier des documents officiels, etc. En outre, le web offre la possibilité de transmettre des données, notamment en créant des sites ou blogs, ou d'exécuter à distance des applications[1468].

[1464] GHERNAOUTI-HÉLIE, DUFOUR, p. 87; GRIESE, SIEBER, p. 43-63.

[1465] GHERNAOUTI-HÉLIE, DUFOUR, p. 91-92; GLESS, p. 15; MÉTRAILLER, SCHURTZ-TAYLOR, p. 28-30.

[1466] Supra Partie II, Chapitre 3, I, A, n° 1101 ss.

[1467] GHERNAOUTI-HÉLIE, DUFOUR, p. 91.

[1468] BONDALLAZ, protection des personnes, p. 29-30

1920 Tous ces services communicationnels ont ouvert la voie à de nouvelles modalités de perpétration des infractions, particulièrement en ce qui concerne la pornographie, la fraude et le blanchiment d'argent[1469]. En outre, étant ouvert à tous et facilement accessible, ce moyen de communication ou de recherche d'informations s'est rapidement démocratisé. C'est pourquoi, pour combattre les nouvelles criminalités liées à l'Internet et pour obtenir des informations précieuses, des indices et/ou des éléments probatoires, l'autorité pénale s'est servie de cette technologie pour surveiller des suspects, des récidivistes, voire pour prévenir la perpétration d'infractions.

b. L'identification des appareils électroniques sur le réseau

i. Le protocole TCP/IP et l'adresse IP

a) Les notions techniques

1921 Sur Internet les ordinateurs communiquent entre eux grâce au protocole TCP/IP qui utilise des adresses numériques ou adresses IP[1470]. Sans adresse IP, il n'est pas possible, pour les ordinateurs, d'échanger ou d'acheminer des paquets de données *via* le réseau Internet. A noter que chaque paquet de données émis contient l'adresse IP de l'émetteur et du destinataire.

1922 Les adresses IP se composent de quatre nombres entre 0 et 255 séparés par un point. Les deux premiers nombres caractérisent le pays et la ville d'origine, les deux suivants identifient le lieu de domicile et le nom du destinataire. Ainsi, il est possible de localiser sur le réseau et d'identifier l'ordinateur ou l'appareil connecté.

1923 Généralement, les adresses IP sont attribuées temporairement – adresses IP dynamiques qui se renouvellent tacitement après trente jours – par les fournisseurs d'accès Internet[1471]. Grâce aux journaux de "logs" créés et conservés par ces fournisseurs d'accès, il est alors possible d'obtenir l'identité du possesseur de l'adresse IP considérée. Normalement, cette méthode d'identification est fiable, dès lors qu'une seule connexion n'est théoriquement possible par adresse IP au même instant[1472].

[1469] CONTAT, MÜLLER, p. 311 et 333; SOULLIERE, p. 21.

[1470] BONDALLAZ, protection des personnes, p. 511; SEEGER, p. 267.

[1471] BONDALLAZ, protection des personnes, p. 253; ROTH Simon, n° 4; SOULLIERE, p. 21.

[1472] Infra Partie II, Chapitre 3, III, A, 5, b, iii, n° 2158-2159.

b) L'adresse IP est-elle une donnée personnelle?

1924 Une adresse IP est une ressource d'adressage qui n'est en tant que telle par forcément une donnée personnelle, puisqu'elle ne permet pas d'identifier par elle-même l'utilisateur. En effet, si "*l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre, on ne peut guère parler de possibilité d'identification.*"[1473].

1925 Le Tribunal fédéral a dans un arrêt récent déterminé à quelles conditions une adresse IP peut être qualifiée de donnée personnelle au sens de l'art. 3 let. a LPD (et art. 4 let. a LIPAD/GE par analogie).

1926 En accord avec la doctrine, la Cour a différencié le cas des adresses IP statiques qui sont souvent répertoriées dans des annuaires, et le cas des adresses IP dynamiques qui demandent le concours du fournisseur d'accès pour identifier l'utilisateur[1474]. Dans le premier cas, il ne fait nul doute qu'il est possible d'identifier facilement l'utilisateur. L'adresse IP est donc une donnée personnelle (art. 3 let. a LPD et art. 4 let. a LIPAD). Dans le second cas, il suffit que le détenteur de l'information puisse relier la donnée à une personne déterminée pour reconnaître la qualité de donnée personnelle à l'adresse numérique[1475].

1927 Dans le cadre d'une action pénale, l'adresse IP permet de recueillir auprès du fournisseur d'accès l'identité de l'utilisateur du raccordement Internet (art. 27 al. 1 let. a OSCPT). Ainsi, qu'elle soit statique ou dynamique, il s'agit d'une donnée personnelle[1476].

ii. L'adresse MAC

1928 L'adresse MAC est l'identifiant physique sis dans une carte réseau ou une interface réseau similaire. Elle est constituée de six nombres composés de deux chiffres ou lettres. Les trois premiers nombres identifient le constructeur de la carte et les trois suivants identifient la carte réseau elle-même.

[1473] ATF 136 II 508, 513-514 = JdT 2011 II 446, 451; MEIER P., p. 208; Message, LPD, p. 452; ROSENTHAL, JÖHRI, art. 3 N 23 et 40.

[1474] ATF 136 II 508, 514-515 = JdT 2011 II 446, 451-452; ROSENTHAL, JÖHRI, art. 3 N 11, 18 ss et 27; WEBER, FERCSIK SCHNYDER, p. 577-579.

[1475] ROSENTHAL, JÖHRI, art. 3 N 11, 20 et 27; WEBER, FERCSIK SCHNYDER, p. 583.

[1476] ATF 136 II 508, 515-516 = JdT 2011 II 446, 452-453; ROSENTHAL, JÖHRI, art. 3 N 27; WEBER, FERCSIK SCHNYDER, p. 577.

1929 Chaque carte réseau a normalement sa propre adresse MAC unique car inscrite physiquement dans l'interface[1477]. Ainsi, il est possible d'identifier individuellement chaque carte connectée sur un réseau.

c. Les supports informatiques

1930 Avec l'évolution technologique, l'écrit manuscrit a, peu à peu, été remplacé – tout du moins en partie – par l'écrit informatisé. De même, les photographies papiers ou autres documents sont dorénavant souvent sauvegardés numériquement.

1931 Si une lettre, un écrit, une image, une bande audio, etc. peuvent servir comme moyen de preuve, il ne fait nul doute que leur forme numérisée peut l'être aussi. Par conséquent, l'administration de la preuve informatique est un enjeu croissant au vu du nombre de données entreposées, recueillies ou traitées au moyen des supports électroniques.

1932 Les notions de "*données*" ou de "*supports informatiques*" se définissent largement. Ainsi, une donnée peut être un fichier écrit, une image, l'historique internet, l'historique de messagerie, un message email, un cookie, un temporaire internet, un historique GPS, etc. En outre, l'information utile ou la donnée peut provenir de divers supports électroniques et être éparpillée dans d'innombrables sources: disque dur interne, support amovible, CD, bande de sauvegarde, etc.[1478].

1933 Dans le cadre de notre étude, nous nommerons donc "*fichier informatique*" ou "*dossier informatique*", tout document électronique ou numérique stocké sur un support informatique qui peut être utile à la procédure pénale et/ou être utilisé comme preuve.

3. Le cadre juridique

a. Les droits fondamentaux, les libertés et leur protection

1934 Notre étude se scinde en trois moyens d'investigation distincts permettant la récolte d'indices ou de preuves: la surveillance sur Internet, la surveillance de l'accès Internet et la perquisition des documents.

[1477] Infra Partie II, Chapitre 3, III, A, 5, b, iii, n° 2160-2161.

[1478] BUQUET, p. 337-338; eDiscovery, KPMG, disponible sur : http://www.kpmg.ca [consulté le 08.05.2016].

1935 Dans le cadre des atteintes potentielles aux droits fondamentaux, il existe peu de différence entre ces méthodes. En tant que moyens de contrainte, elles créent toutes une ingérence à la vie, à la sphère privée et à l'autodétermination informationnelle (art. 8 § 1 CEDH, art. 17 § 1 Pacte II et art. 10 et 13 al. 1-2 Cst).

1936 Afin d'éviter toutes redondances, la surveillance de l'accès Internet faisant partie intégrante de la surveillance de la correspondance par poste et télécommunication, il est suffisant de nous référer à l'analyse précédemment effectuée[1479]. Au surplus, l'atteinte à la vie privée et/ou le droit au respect du domicile ayant également déjà fait l'objet d'une étude[1480], nous traitons exclusivement la reconnaissance de l'ingérence aux droits fondamentaux créée par la surveillance sur Internet et la perquisition. Nous ne revenons donc pas sur le contenu précis des droits fondamentaux atteints ou sur les conditions de restrictions.

i. La surveillance sur Internet et l'atteinte aux libertés personnelles

1937 La surveillance sur Internet peut être passive – simple observation – ou active – investigation secrète ou recherche secrète[1481].

a) En cas d'observation

1938 Le Tribunal fédéral[1482] et la Cour européenne des droits de l'homme[1483] ont reconnu que l'observation était une mesure d'investigation qui causait une atteinte à la vie privée. La doctrine précise encore qu'il faut évaluer la gravité de l'ingérence à ce droit fondamental en fonction de la prolongation dans le temps de l'observation[1484]. Par ailleurs, la Cour européenne des droits de l'homme a communiqué des affaires aux gouvernements incriminés par des requêtes en ce qui concerne la violation de l'art. 8 CEDH par une mesure d'observation, si bien que, dans un futur plus ou moins proche, la Cour de Strasbourg sera

[1479] Supra Partie II, Chapitre 3, I, A, 2, a, n° 1115 ss.

[1480] Supra Partie II, Chapitre 3, I, A, 2, a, n° 1115 ss; Supra Partie II, Chapitre 3, I, B, 2, a, n° 1452 ss; Supra Partie II, Chapitre 3, II, C, 1, n° 1714 ss.

[1481] Infra Partie II, Chapitre 3, III, A, 3, c, i, n° 1971 ss.

[1482] ATF 140 I 381, 385-386 et 390.

[1483] Affaire *Copland c. Royaume-Unis*, arrêt du 3 avril 2007, 62617/00, § 44 ss.

[1484] GISLER, p. 87-88; THOMANN, p. 290; VEST, p. 668-670; ZALUNARDO-WALSER, p. 50-52. Supra Partie II, Chapitre 3, II, C, 2, a, ii, a), n° 1745 ss.

invitée à délimiter la gravité de l'ingérence et les conditions à remplir pour autoriser l'atteinte aux droits fondamentaux[1485].

1939 En suivant ce courant doctrinal, le législateur a décidé d'intégrer l'observation dans le catalogue des mesures de contrainte au sein du Code de procédure pénale. Par nature, ces mesures sont propres à porter atteinte aux droits fondamentaux[1486], spécifiquement à la liberté personnelle et à l'autodétermination informationnelle. Dès lors, il ne nous semble pas erroné de voir, dans la volonté du législateur fédéral, la reconnaissance implicite de l'existence d'une ingérence à la vie privée lorsque l'autorité pénale observe un événement ou une personne sur la voie publique[1487].

b) En cas d'investigation secrète et de recherches secrètes

1940 L'investigation secrète consiste à nouer des contacts avec une personne soupçonnée dans le but de constater et de prouver la commission d'une infraction sans que le policier ne soit reconnaissable[1488].

1941 Lors des investigations secrètes sur Internet, même si l'utilisation de pseudonyme est l'usage dans les forums de discussion, il n'en reste pas moins qu'un policier qui n'énonce pas être un représentant des forces de l'ordre est un agent infiltré[1489]. Ainsi, la personne surveillée converse avec un tiers dont il ne connaît ni les réelles motivations, ni la réelle identité.

1942 Par conséquent, la doctrine considère que l'investigation secrète restreint la liberté de choix de la personne surveillée[1490]. En étant trompée et/ou en faisant erreur sur l'identité de son interlocuteur, elle n'est plus libre de décider à qui elle désire fournir des informations qu'elle souhaite confidentielles. Dès lors, les libertés personnelles et le droit à l'autodétermination informationnelle sont mis en péril lors de l'utilisation de ce moyen d'investigation. A noter que cette ingérence aux droits fondamentaux est qualifiée par la doctrine comme grave[1491].

[1485] *Bureau of investigation journalism and Alice Ross c. Royaume-Uni,* transmis au Gouvernement le 5 janvier 2015, 62322/2014; *Big Brother Watch et autres c. Royaume-Uni*, transmis au Gouvernement le 7 janvier 2014, 58179/13.

[1486] ATF 135 I 113, 117 = JdT 2009 IV 104, 107; ATF 136 I 87, 96-97 = JdT 2010 I 367, 374-375; CR-CPP-VIREDAZ, JOHNER, art. 196 N 4; HAUSER, SCHWERI, HARTMANN, p. 323; Message, CPP, p. 1196; SCHMID, Praxiskommentar, art. 196 N 1; StPO-HUG, SCHEIDEGGER, art. 196 N 2.

[1487] En accord avec: BSK-StPO-KATZENSTEIN, EUGSTER, art. 282 N 3; CR-CPP-GUÉNIAT, HAINARD, art. 282 N 2.

[1488] ATF 134 IV 266, 275 = JdT 2008 IV 35, 49; ATF 135 I 169, 171 = JdT 2010 I 191, 193.

[1489] ATF 134 IV 266, 277-278 = JdT 2008 IV 35, 51.

[1490] ATF 112 Ia 18, 21 = JdT 1986 IV 116, 117-118; BSK-StPO-KNODEL, art. 286 N 1; HAUSER, SCHWERI, HARTMANN, p. 386-388; Message, CPP, p. 1238; VETTERLI, Verdeckte Ermittlung, p. 367.

[1491] BSK-StPO-KNODEL, art. 286 N 1; VETTERLI, Verdeckte Ermittlung, p. 367.

ii. La perquisition des documents, l'atteinte à la vie privée et au droit au respect du domicile

1943 La perquisition se définit comme la recherche approfondie et minutieuse de tous les éléments de preuve et d'indices susceptibles d'intéresser la manifestation de la vérité[1492]. Au cours d'une fouille d'un individu (art. 249-250 CPP) ou d'une perquisition de locaux (art. 244-245 CPP), l'autorité pénale est régulièrement confrontée à des documents et des enregistrements dont elle ignore le contenu, mais serait désireuse de l'apprendre. Elle peut également connaître l'existence d'un document ou d'un enregistrement déterminé et vouloir l'obtenir aux fins de la récolte d'indices et/ou d'éléments de preuve[1493].

1944 Les documents électroniques sont comparables aux écrits manuscrits ou aux enregistrements audio ou vidéo. Dès lors, ils contiennent des données et des informations personnelles, sensibles et/ou secrètes[1494].

1945 Ainsi, la perquisition de documents et d'enregistrements est une mesure d'investigation de nature à porter atteinte gravement à la sphère privée de la personne prévenue ou de tiers, et à l'autodétermination informationnelle qui protège, notamment, les secrets et les données personnelles en conférant au titulaire un droit de contrôle sur celles-ci[1495].

1946 En outre, une ingérence au droit au respect du domicile est inévitable. En effet, pour perquisitionner un lieu, l'autorité de poursuite pénale est dans l'obligation d'entrer dans des locaux privés[1496]. Concernant spécifiquement la perquisition des documents ou des enregistrements, un ordinateur ou tout autre support informatique sont conservés au sein

[1492] CR-CPP-CHIRAZI, art. 244 N 1; PIQUEREZ, MACALUSO, p. 1329.

[1493] CR-CPP-CHIRAZI, art. 246 N 1; StPO-KELLER, art. 246 N 1.

[1494] ATF 130 II 193, 195-196 = JdT 2005 IV 309, 310-312; ATF 137 IV 189, 194; BSK-StPO-THORMANN, BRECHBÜHL, art. 246 N 1; HAUSER, SCHWERI, HARTMANN, p. 353-354; OBERHOLZER, Strafprozessrechts, p. 387; Polizeiliche Ermittlung-ARMBRUSTER, p. 356.

[1495] ATF 133 I 77, 81 = JdT 2008 I 418, 422; ATF 136 I 87, 91-92; ATF 138 I 256, 258; CourEDH, Affaire *Ernst et autres c. Belgique*, arrêt du 15 juillet 2003, 33400/96, § 110; CourEDH, Affaire *Petri Sallinen et autres c. Finlande*, arrêt du 27 septembre 2005, 50882/99, § 70-72; CourEDH, Affaire *Wieser et Bicos Beteiligungen GMBH c. Autriche*, arrêt du 16 octobre 2007, 74336/01, § 44; CourEDH, Affaire *Robathin c. Autriche*, arrêt du 03 juillet 2012, 30475/06, § 39; BSK-StPO-THORMANN, BRECHBÜHL, art. 246 N 1; Message, CPP, 1220; OBERHOLZER, Strafprozessrechts, p. 387; SCHMID, Handbuch, p. 461-462; SCHMID, Praxiskommentar, art. 244 N 1; StPO-KELLER, art. 246 N 2.

[1496] CourEDH, Affaire *Gillow c. Royaume-Uni*, arrêt du 24 novembre 1986, 9063/80, § 46; CourEDH, Affaire *Société Colas Est et autres c. France*, arrêt du 16 avril 2002, 37971/97, § 40-42; CourEDH, Affaire *Petri Sallinen et autres c. Finlande*, arrêt du 27 septembre 2005, 50882/99, § 70-72; CourEDH, Affaire *Wieser et Bicos Beteiligungen GMBH c. Autriche*, arrêt du 16 octobre 2007, 74336/01, § 43.

même d'une propriété privée. Ainsi, le droit au respect du domicile est indirectement touché par ce type de perquisition.

1947 Relevons encore que l'effectivité de l'autodétermination informationnelle dans le cadre des données informatiques passe notamment par la reconnaissance du droit à la protection du domicile électronique. Ce droit garantit la confidentialité et l'intégrité des informations stockées par les usagers ou par des tiers sur un espace numérique privé ou individuel[1497]. Lorsqu'une autorité pénale s'introduit dans un support informatique aux fins de récolter des données ou d'en connaître le contenu, ce comportement est comparable à la violation par cette même autorité du domicile physique protégé par les normes conventionnelles, constitutionnelles et pénales[1498].

b. La protection du Code pénal

1948 La surveillance sur Internet, de l'accès Internet et la perquisition de document à distance ou directement sur un espace de stockage informatique sont, dans certaines circonstances, pénalement répréhensibles. Diverses infractions sont donc à considérer.

i. La soustraction de données (art. 143 CP)

1949 Les données traitées par un ordinateur ne sont ni des choses ni des valeurs patrimoniales, c'est pourquoi le législateur a adopté l'art. 143 CP pour réprimer spécifiquement la soustraction des données informatiques.

1950 L'objet de l'infraction doit être une donnée, soit une information qui peut faire l'objet d'une communication et qui est stockée sur un ordinateur ou un support électronique similaire, ou qui est transférée[1499].

1951 La disposition légale requiert que la donnée ait comme qualité particulière "*[d'être] spécialement protégée*". Dès lors, les données accessibles au public – nous pensons notamment aux informations inscrites sur un forum, un blog ou toutes autres pages internet, ou les données stockées sur un support informatique qui ne sont ni cryptées, ni

[1497] BONDALLAZ, protection des personnes, p. 351; CONSEIL DE L'EUROPE, Document CM (2004) 41, § 38.

[1498] TRÜEB, p. 65.

[1499] DONATSCH, Strafrecht, p. 194; MÉTILLE-RPS, p. 290; STRATENWERTH, JENNY, BOMMER, p. 358; TRECHSEL, PIETH-TRECHSEL, CRAMERI, art. 143 N 1.

protégées par un mot de passe –, ou contenues dans une base de données accessible moyennant un paiement sont par conséquent exclues[1500].

1952 Ainsi, le comportement d'un agent infiltré ou d'un observateur sur internet qui recueille des données directement en surveillant un groupe de discussion ou une page internet similaire n'est pas pénalement typique au sens de l'art. 143 CP. De même, l'autorité pénale qui perquisitionne un support informatique non-protégé réalise un comportement pénalement indifférent au sens de ce même article.

1953 Reste à déterminer si, lorsque les fichiers informatiques sont cryptés, sont protégés par un mot de passe ou sont spécifiquement équipés d'un programme de protection, la perquisition ou la prise de connaissance à distance à l'aide d'un cheval de Troie est constitutive de l'infraction.

1954 Le comportement punissable consiste dans le fait à se procurer une donnée informatique par n'importe quel moyen. Il suffit donc que l'auteur puisse en prendre connaissance afin de pouvoir l'utiliser[1501].

1955 Cependant, même si objectivement le comportement de l'autorité pénale qui perquisitionne des documents ou les récupère à distance, ou le comportement d'un particulier qui désire obtenir des preuves correspondent à la définition de l'art. 143 CP, l'infraction requiert le dessein d'enrichissement illégitime. Dès lors, la simple curiosité, la simple malveillance et/ou la récolte d'indices ou de preuves n'entrent pas dans le cadre de cet article à défaut d'accomplir le dol spécial[1502].

ii. L'accès indu à un système informatique (art. 143bis CP)

1956 Lorsqu'une autorité de poursuite pénale veut s'introduire dans un espace de stockage – peu importe le type tant que le système repose sur un moyen informatique – qui est sécurisé par un mot de passe ou dont les informations sont cryptées, elle commet *a priori* un acte typiquement contraire au droit pénal au sens de l'art. 143*bis* CP[1503]. A noter que la

[1500] MÉTILLE-RPS, p. 291; STRATENWERTH, JENNY, BOMMER, p. 360-361; TRECHSEL, PIETH-TRECHSEL, CRAMERI, art. 143 N 6.

[1501] DONATSCH, Strafrecht, p. 197; STRATENWERTH, JENNY, BOMMER, p. 361-362; TRECHSEL, PIETH-TRECHSEL, CRAMERI, art. 143 N 7.

[1502] TRECCANI, p. 218.

[1503] DONATSCH, Strafrecht, p. 199; MÉTILLE-RPS, p. 298; STRATENWERTH, JENNY, BOMMER, p. 363; TRECHSEL, PIETH-TRECHSEL, CRAMERI, art. 143*bis* N 6.

jurisprudence a reconnu qu'un tiers employant un mot de passe pour accéder au compte email d'autrui pénètre simultanément dans le système informatique lui-même et viole donc cette norme[1504].

1957 Cependant, l'art. 143*bis* CP spécifie que l'accès indu au système informatique appartenant à autrui doit être réalisé sans droit. En cas d'investigation répressive, l'art. 245 CPP prévoit la perquisition des systèmes informatiques. Le comportement de l'autorité pénale est par conséquent autorisé. En cas d'investigation préventive, l'art. 18*m* P-LMSI II[1505] vise expressément à rendre non punissable un tel comportement. En revanche, jusqu'à l'acceptation du P-LMSI II et de son entrée en vigueur, la loi fédérale actuelle ne permet pas l'investigation préventive. Au surplus, rappelons encore que les normes cantonales manquent en la matière[1506].

1958 Concernant spécifiquement l'utilisation d'un cheval de Troie pour recueillir les données, nous renvoyons à ce qui a été énoncé à l'aune de l'interception des communications VoIP et de la violation de l'art. 143*bis* CP[1507].

1959 Quant à la soustraction de données par des particuliers, le comportement est typique, mais peut être justifié par l'état de nécessité ou la légitime défense. En outre, le principe de la *Beweisnotstand* est également applicable.

iii. La violation des art. 179 à 179quater et 179novies CP en cas de surveillance par l'autorité

1960 En ce qui concerne les données enregistrées sur un support informatique issues d'une communication électronique, nous devons nous déterminer sur la typicité du comportement d'une autorité pénale ou d'un particulier au regard des art. 179 ss CP.

1961 Au sens de l'art. 179 CP, la commission de l'infraction suppose l'ouverture d'un pli ou d'un colis. Dès lors, l'objet de l'infraction doit être fermé. Nous l'avons vu, les emails ou autres données – protégées par un mot de passe ou non – en transit ou stockés dans un ordinateur ne font pas partie de la définition de l'objet de l'infraction faute d'être "fermés"[1508]. Le

[1504] ATF 130 III 28, 32-33; TF 6B_456/2007 du 18 mars 2008, c. 4.3.

[1505] Projet de loi fédérale instituant des mesures visant au maintien de la sûreté intérieure – Moyens spéciaux de recherche d'informations (P-LMSI II).

[1506] Supra Partie II, Chapitre 3, I, A, 4, c, ii, n° 1355 ss.

[1507] Supra Partie II, Chapitre 3, I, A, 4, c, i, b) et c), n° 1307 ss et 1328 ss.

[1508] Supra Partie II, Chapitre 3, I, A, 2, b, n° 1134.

comportement de l'autorité pénale ou d'un particulier n'est donc pas constitutif de l'infraction de l'art. 179 CP lorsqu'ils ouvrent des fichiers ou enregistrements informatiques.

1962 En vertu de l'art. 179*bis* CP, la protection pénale concerne les "*conversations*". Par ce terme, il faut entendre un entretien oral[1509]. Ainsi, un échange de messages électroniques à l'aide d'un logiciel de messagerie – par l'entremise d'emails ou d'un groupe de discussion sur Internet – ne peut pas donner lieu à cette infraction. Par conséquent, l'autorité pénale ou un particulier qui enregistre une communication écrite à l'aide d'un historique de conversations ou lit des messages écrits à l'aide d'un moyen informatique ne commet pas d'action typique au sens de l'art. 179*bis* CP.

1963 L'art. 179*ter* CP reprenant largement les principes de l'art. 179*bis* CP, à défaut de conversation orale, les éléments constitutifs objectifs de l'infraction ne sont pas non plus réalisés.

1964 Au sens de l'art. 179*quater* CP, les images relevant du domaine secret ou privé sont spécifiquement protégées[1510]. Le comportement punissable peut se présenter sous la forme d'une observation avec un appareil de prise de vues ou de la fixation sur un porteur d'images. Dans le cadre de notre sujet, il faut déterminer si la fonction *print screen* qui permet d'effectuer une capture d'écran et de l'enregistrer sur un disque dur, et/ou si l'enregistrement sur un support informatique d'une image ou d'une vidéo tombe sous le coup de cette disposition légale.

1965 Le législateur a formulé l'art. 179*quater* CP de façon à permettre son application au gré de l'évolution des nouvelles technologies[1511]. Thomas Legler estime, notamment, que le disque dur d'un ordinateur contenant des images sous forme numérique constitue un porteur d'images[1512]. En conséquence, il nous semble cohérant d'affirmer qu'une personne effectuant une capture d'écran ou enregistrant des images provenant d'un groupe de discussion, d'un email ou de toute autre messagerie électronique réalise l'action incriminée.

1966 N'oublions toutefois pas que ce comportement n'est pénalement typique que dans l'hypothèse où le fait fixé sur le porteur d'images relève du domaine secret ou privé. Dès lors, toutes les informations obtenues par le biais d'un groupe de discussion ouvert au public ne relèvent

---

[1509] DONATSCH, Strafrecht, p. 401-402; STRATENWERTH, JENNY, BOMMER, p. 266-267; TRECHSEL, PIETH-TRECHSEL, LIEBER, art. 179*bis* N 2.

[1510] Pour la définition de domaine privé ou secret, voir: Supra Partie II, Chapitre 3, I, B, 2, b, n° 1488 ss.

[1511] HURTADO POZO, art. 179*quater* N 2265; SCHUBARTH, Strafrecht, art. 179*quater* N 23.

[1512] LEGLER, p. 147.

pas de ces domaines, puisqu'elles peuvent être perçues par tout un chacun. En revanche, les messages privés, les discussions sur un forum qui restreint l'accès à certaines personnes, les emails, les discussions instantanées privées, etc. fournissent des informations qui peuvent relever du domaine privé ou secret.

1967 Concernant l'application de l'art. 179*novies* CP, elle demande à ce que les données soient soustraites d'un fichier – soit d'un ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée – au sens de l'art. 3 let. g LPD. Dès lors, lorsqu'un particulier ou l'autorité pénale soustrait des données sous forme de simple fichier informatique, la disposition légale n'est pas applicable. En revanche, lorsqu'il s'agit de récupérer des données en les soustrayant d'un fichier au sens de l'art. 3 let. g LPD et qu'elles ont le caractère de données personnelles sensibles (art. 3 let. c LPD) ou de profil de la personnalité (art. 3 let. d LPD), alors le comportement est constitutif de l'infraction.

1968 En toute hypothèse, si le comportement du particulier ou de l'autorité pénale est typique, un motif justificatif – acte autorisé par la loi, légitime défense ou état de nécessité – peut rendre licite le comportement.

c. Les normes justifiant l'atteinte aux droits fondamentaux

1969 Dans le cadre des investigations effectuées par la police ou par la direction de la procédure, la procédure pénale autorise un certain nombre de surveillances.

1970 En ce qui concerne la surveillance préventive par une autorité sur Internet, de l'accès Internet ou de l'introduction à distance dans un système informatique pour prendre connaissance des fichiers, et sur ces mêmes comportements effectués par les particuliers, nous nous limitons aux développements précédents qui valent *mutatis mutandis* et à l'énonciation de l'introduction de l'art. 18*m* P-LFIS II[1513].

1971 Nous axons donc la présentation du cadre légal sur les dispositions de procédure pénale applicables en cas de surveillance répressive.

[1513] Supra Partie II, Chapitre 3, I, A, 2, d, n° 1226 ss; Supra Partie II, Chapitre 3, I, A, 4, c, ii, n° 1355 ss; Supra Partie II, Chapitre 3, II, C, 2, a, iii, n° 1770-1771.

i. En cas de surveillance sur Internet

1972 Pour lutter contre le crime organisé, la criminalité informatique – en rapport avec la pornographie ou avec des sites présentant un caractère pernicieux – ou pour obtenir des informations *via* le réseau Internet, les autorités pénales doivent pouvoir effectuer des surveillances sur Internet. En pratique, un service ou une division spécialisée des polices cantonales effectue les recherches liées aux actes délictuels considérés et aide les autres services de police dans le cadre des recherches informatiques au moyen d'outils et de logiciels spécifiques.

1973 Pour ce qui touche à la recherche sur Internet d'informations utiles à l'enquête pénale et pouvant servir de preuve, la police peut adopter un comportement passif en se limitant à la recherche et à la lecture d'informations, ou actif en participant aux discussions ou en entrant en contact avec un individu soupçonné.

1974 Pour différencier l'observation d'une part et l'investigation secrète, qui actuellement comprend deux volets : l'investigation secrète au sens stricte et les recherches secrète, d'autre part, il nous faut nous référer à la jurisprudence rendue en application de l'aLFIS abrogée par l'entrée en vigueur du CPP qui reprend – avec quelques modifications – les dispositions de cette loi aux art. 285a ss CPP[1514] et la jurisprudence rendue à l'encontre des dispositions cantonales de surveillance préventive[1515].

1975 Dans un arrêt de principe[1516], le Tribunal fédéral avait défini le champ d'application de l'aLFIS. Contrairement à l'avis de la doctrine majoritaire[1517] et à la jurisprudence cantonale zurichoise[1518], le Tribunal fédéral avait qualifié l'investigation secrète de manière large. Il s'agit de toute activité de contact par un fonctionnaire de police qui n'est pas reconnaissable comme tel avec un suspect aux fins d'élucider une infraction.

1976 Ainsi, l'investigation secrète n'imposait, selon le Tribunal fédéral, pas l'utilisation d'une identité d'emprunt, ni une certaine intensité relative à la durée de la mesure[1519]. Cette notion est celle reprise par le législateur aux art. 285a ss CPP incluant l'investigation secrète et les recherches secrète. En reprenant cette jurisprudence, nous pouvons en conclure qu'il est

[1514] Ancienne loi fédérale sur l'investigation secrète (aLFIS).

[1515] ATF 140 I 381, 384 et 385.

[1516] ATF 134 IV 266 = JdT 2008 IV 35.

[1517] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 276; HANSJAKOB, verdeckte Ermittlung, p. 97 ss; JOSITSCH, Strafprozessrechts, p. 152; SCHMID, Praxiskommentar, art. 286-298 N 3 ss.

[1518] OGer ZH, ZR 107 (2008) 15, p. 51 ss; OGer ZH, ZR 103 (2004) 41, p. 167 ss.

[1519] ATF 134 IV 266, 275 et 277 = JdT 2008 IV 35, 49 et 50-51; ATF 140 I 381, 384-385.

nécessaire que la police ne se contente pas d'observer dans le cadre des deux modes de contraintes précités. La police doit communiquer avec le suspect peu importe le moyen utilisé (message sur un forum, "*chat room*", etc.)[1520].

1977 Par conséquent, lorsque l'autorité suit simplement une communication entre des tiers sur Internet, sans intervenir, le comportement est qualifié d'observation (art. 282 ss CPP) ou de surveillance policière. En revanche, lorsque l'autorité participe secrètement à une communication sur Internet, la procédure relative à l'investigation secrète et/ou aux recherches secrètes s'appliquent (art. 285a ss CPP), étant relevé qu'avec l'introduction des nouvelles dispositions (art. 285a et 296a ss CPP), l'investigation secrète requérant une identité d'emprunt attesté par un titre ne répond plus aux prérogatives du cyberespace où un acte authentique n'est pas utile pour s'identifier[1521].

a) L'observation

1978 A la lecture de la jurisprudence, nous avons constaté que le Tribunal fédéral différencie l'observation et l'investigation secrète. La distinction entre l'observation et la surveillance policière est plus délicate[1522].

1979 En raison de la nature de la surveillance sur Internet, il nous faut effectuer cette distinction. En effet, l'activité déployée par l'autorité pénale sur Internet peut être spontanée et/ou ponctuelle, ou systématique et d'une certaine intensité dans le temps[1523]. Contrairement à la vidéosurveillance répressive – par exemple –, il arrive fréquemment qu'un agent de police ne fasse que passer sur un forum sans avoir une activité de surveillance réelle.

1980 La surveillance policière est ouverte ou secrète, préventive ou répressive, intervient à court terme et ne fait pas l'objet d'enregistrements systématiques. Il s'agit d'une mesure de police standard qui ne relève pas des art. 282 ss CPP, dès lors qu'elle intervient de manière fortuite ou spontanée, et non pas suite à un mandat de surveillance systématique[1524].

[1520] ATF 134 IV 266, 275 = JdT 2008 IV 35, 49; ATF 135 I 169, 171 = JdT 2010 I 191, 193; RUDAZ, n° 2.

[1521] ATF 134 IV 266, 277 = JdT 2008 IV 35, 50-51; ATF 140 I 381, 385; RVJ 2012 p. 340, p. 344-345; TF 6B_568/2009 du 8 octobre 2010, c. 3.3; TF 6B_837/2009 du 8 mars 2010, c. 3.4; GLESS, p. 15; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 471 et 499; SCHMID, Praxiskommentar, art. 286-298 N 4 ss.

[1522] ATF 140 I 381, 390.

[1523] ATF 140 I 381, 390; CR-CPP-GUÉNIAT, HAINARD, art. 282 N 3; MOREILLON, PAREIN-REYMOND, art. 282 N 3; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 472. Infra Partie II, chapitre 3, III, A, 3, c, i, b), 1, n° 1987 ss.

[1524] CR-CPP-GUÉNIAT, HAINARD, art. 282 N 2-3; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 238; PITTELOUD, p. 459; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 472; ZALUNARDO-WALSER, p. 47 ss.

1981 L'observation s'effectue dans un but de poursuite pénale, est dirigée contre une personne, une chose ou un objet déterminé et est planifiée à long terme[1525].

1982 Par conséquent, lorsqu'une surveillance sur Internet est effectuée, il faut analyser les circonstances de l'activité déployée pour déterminer s'il s'agit d'une simple surveillance policière ou d'une observation.

1983 Généralement, dans le dessein d'obtenir des indices et/ou des preuves, la surveillance est étendue dans le temps et vise un individu déterminé même caché derrière un pseudonyme. Dès lors, nous avons fréquemment affaire à une preuve provenant d'une activité d'observation qui n'est exploitable que si elle a été obtenue dans le respect des conditions procédurales.

1984 A ce sujet, les dispositions relatives à l'observation (art. 282 et 283 CPP) ayant déjà fait l'objet de commentaires dans le cadre de la vidéosurveillance répressive effectuée par les autorités sur domaine public, nous nous référons à cette analyse concernant la procédure[1526].

b) L'investigation secrète

1985 Originellement, lors de l'entrée en vigueur du Code de procédure pénale suisse le 1er janvier 2011, l'investigation secrète était réglementée aux art. 286 et ss CPP.

1986 Depuis l'entrée en vigueur des dispositions sur les recherches secrètes (art. 298a ss CPP), l'art. 285a CPP vient compléter les dispositions légales précitées qui sont incontestablement des bases légales formelles nécessaires pour justifier l'atteinte grave aux droits fondamentaux causée par cette mesure d'investigation[1527].

1. L'investigation secrète

1987 Avant l'entrée en vigueur de l'art. 285a CPP le 1er mai 2013, la jurisprudence considérait que toute prise de contact avec un suspect aux fins d'élucidation d'une infraction par un fonctionnaire de police qui n'est pas reconnaissable comme tel devait être qualifiée

[1525] BSK-StPO-KATZENSTEIN, EUGSTER, art. 282 N 1 ss; Message, CPP, p. 1235.

[1526] Supra Partie II, Chapitre 3, I, B, 2, c, ii, d, n° 1556 ss.

[1527] CR-CPP-JEANNERET, RYSER, art. 286-289 N 19; OBERHOLZER, Strafprozessrechts, p. 434-435; SCHMID, Strafprozessrecht, p. 295-296; ZALUNARDO-WALSER, p. 126.

d'investigation secrète au sens de l'aLFIS, indépendamment des moyens mis en œuvre pour tromper le suspect et de l'intensité de l'intervention[1528].

1988 Actuellement, l'art. 285a CPP définit "*l'investigation secrète comme une mesure consistant pour un membre du corps de police ou des personnes engagées à titre provisoire pour accomplir des tâches de police, à infiltrer un milieu criminel pour élucider des infractions particulièrement graves, en nouant un contact avec des individus et en instaurant avec eux une relation de confiance particulière par le biais d'actions ciblées menées sous le couvert d'une fausse identité dont ils sont munis dans la durée et qui est attestée par un titre (identité d'emprunt)*".

1989 Cette disposition limite l'investigation secrète telle que connue originellement, soit avant l'édiction de dispositions sur les recherches secrètes, et réduit considérablement son champ d'application.

1990 En premier lieu, contrairement à ce qui prévalait avant le 1er mai 2013 au sens de l'art. 288 al. 1 aCPP, la dotation d'une identité d'emprunt attestée par un titre est obligatoire et non plus laissée à la libre appréciation du ministère public[1529]. En outre, la compétence d'octroyer cette identité d'emprunt revient à la police et non plus au ministère public.

1991 Deuxièmement, l'investigation secrète ne se définit plus par le rôle actif et la prise de contact avec un interlocuteur, mais comme une prise de contact qui s'étend sur la durée. Ainsi, les comportements, même actifs, d'un agent infiltré qui agit spontanément, ponctuellement et sur une courte durée n'entre plus dans le champ d'application de l'investigation secrète.

1992 Deux critiques peuvent être formulées sur cette modification du Code de procédure civile qui à restreindre le champ d'application de l'investigation secrète.

1993 L'une est d'ordre général. A la lecture de l'art. 285a CPP, le texte légal nous laisse penser que ce qui est déterminant pour qualifier la mesure policière d'investigation secrète est l'utilisation dans la durée d'une identité d'emprunt. Cette interprétation littérale est malheureuse.

1994 En effet, d'après nous, ce qui doit qualifier la mesure c'est l'activité déployée et non pas l'usage d'une identité d'emprunt en tant que tel. Dès lors, il serait préférable de modifier le texte pour éviter toute ambiguïté.

[1528] ATF 134 IV 266, c. 3.5 à 3.7 = JdT 2008 IV 35; PERRIER DEPEURSINGE, art. 285*a*, p. 369; PITTELOUD, p. 470.

[1529] ATF 140 I 381, 385.

1995 La deuxième critique vise spécifiquement le cadre de notre étude. Dans le monde virtuel, l'identité d'emprunt se limite bien souvent à un complexe de mensonges sur le nom, le prénom, l'emploi, le lieu d'habitation, etc. de l'agent de police, voire l'envoi d'une fausse photographie.

1996 Par conséquent, la surveillance sur Internet *via*, notamment, des réseaux sociaux ou des forums de discussions, ne nécessite pas l'utilisation d'un acte authentique. L'art. 285a CPP ne semble donc pas adapté à la réalité du cyberespace. La conséquence est qu'à défaut d'identité d'emprunt attestée par un titre, l'une des conditions cumulatives de cette base légale n'est pas remplie, et donc la surveillance sur Internet ne sera jamais ou très rarement qualifiée d'investigation secrète créant des risques considérables pour la protection des droits fondamentaux[1530]. Cette remarque vaut de même en cas de surveillance préventive réalisée avant la commission d'infraction, si tant est que le droit cantonal prévoit une telle surveillance[1531].

2. La notion d'agent infiltré et délimitation

1997 L'investigation secrète nécessite l'introduction dans un environnement criminel – physiquement ou à distance par le biais d'un ordinateur – d'un membre du corps de police suisse ou étrangère (art. 287 al. 1 let. a et 287 al. 3 CPP) ou d'une personne engagée à titre provisoire pour accomplir une tâche de police (art. 287 al. 1 let. b CPP).

1998 Contrairement à ce qui prévalait à l'art. 5 al. 1 aLFIS, le consentement de l'agent infiltré n'est plus expressément prévu. Néanmoins, à la lecture des travaux préparatoires, il ne semble pas que le législateur ait voulu renoncer à cette condition[1532].

1999 Dans le cadre des investigations secrètes, l'agent infiltré – membre du corps de police ou une personne mandatée ayant des connaissances particulières[1533] – agit anonymement à l'aide d'une identité d'emprunt qui résiste à une certaine vérification (art. 288 CPP) dans le dessein de se procurer des moyens de preuves[1534]. Dès lors que l'agent infiltré est doté d'une identité

[1530] Initiative parlementaire 08.458 – Synthèse des résultats, p. 11.

[1531] ATF 140 I 381, 385; RUDAZ, n° 1.

[1532] Dans ce sens: CR-CPP-JEANNERET, RYSER, art. 287 N 13.

[1533] BSK-StPO-KNODEL, art. 287 N 4 ss; CR-CPP-JEANNERET, RYSER, art. 287 N 10; HAUSER, SCHWERI, HARTMANN, p. 386-387; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 279; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 510.

[1534] ATF 140 I 381, 385; TF 1B_123/2008 du 2 juin 2008, c. 2.7; BSK-StPO-KNODEL, art. 288 N 1; JOSITCH, MULLE, p. 494; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 494; RUDAZ, n° 7.

fictive, il peut également bénéficier de la garantie de l'anonymat (art. 288 al. 2 CPP *cum* 151 CPP), sauf si elle est levée par le tribunal des mesures de contrainte en cas d'infraction – vraisemblablement grave[1535] – commise par l'agent (art. 288 al. 3 CPP).

2000 La dotation d'une identité fictive n'est pas obligatoire. Le ministère public est en effet libre d'apprécier les circonstances où elle est requise. Dès lors, un agent infiltré peut agir sous un simple pseudonyme ou avec sa réelle identité[1536].

2001 Relevons encore que l'activité de l'agent infiltré intervient dans le cadre d'une investigation dépendante de l'ouverture d'une instruction pénale. Lorsqu'un membre du corps de police agit avant l'ouverture d'une instruction par le ministère public, il ne s'agit pas d'investigation secrète au sens des art. 285a et ss CPP, mais d'une simple mesure de police, étant précisé que dans cette dernière circonstance, l'intensité d'action et l'intervention individuelle sans identité d'emprunt distingue l'activité ponctuelle d'un policier de celle d'un agent infiltré au sens de l'art. 287 CPP[1537]. Néanmoins, il sied de relever que le droit cantonal peut également différencier l'investigation préventive et la recherche préventive en prévoyant de doter d'une identité d'emprunt le policier[1538]. La différenciation entre la mesure de police et de surveillance dépend alors de la durée de la mesure.

3. Les conditions matérielles

2002 L'autorité compétente pour ordonner une investigation secrète est exclusivement le ministère public (art. 286 al. 1 CPP).

a) L'existence de soupçon de la commission d'une infraction énumérée à l'alinéa 2

2003 Contrairement à ce qui prévalait sous l'aLFIS, l'investigation secrète ne peut être qu'une mesure réactive, ce qui exclut donc son utilisation de manière préventive[1539]. En effet, l'art. 286 al. 1 let. a CPP exige l'existance de soupçons qui laissent présumer qu'une infraction énumérée à l'alinéa 2 a été commise.

1535 BSK-StPO-KNODEL, art. 288 N 25; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 280; SCHMID, Praxiskommentar, art. 288 N 8.

1536 ATF 134 IV 266, 274 = JdT 2008 IV 35, 47-48.

1537 TF 1B_29/2007 du 2 avril 2007, c. 6.1; OGer ZH, ZR 107 (2008) 15, p. 51 ss.

1538 ATF 140 I 381, 384 et 385.

1539 BSK-StPO-KNODEL, art. 286 N 16; CR-CPP-JEANNERET, RYSER, art. 286 N 31; MUGGLI, p. 255; SCHMID, Praxiskommentar, art. 286 N 2.

2004 La solution adoptée par le législateur de créer un catalogue d'infractions est cohérente avec ce qui prévaut pour la surveillance de la correspondance par poste et télécommunication[1540]. En revanche, le catalogue n'est pas identique, dès lors que l'investigation secrète n'est pas utile pour élucider un certain nombre d'infractions et qu'elle n'est admissible que pour des crimes ou délits graves, qualifiés ou poursuivis d'office[1541].

2005 Concernant la qualité des soupçons, l'art. 286 al. 1 let. a CPP ne prévoit pas de "*graves soupçons*" comme à l'art. 269 al. 1 let. a CPP. Au vu de l'intensité de l'atteinte aux droits fondamentaux et du catalogue plus restrictif des infractions concernées, de simples soupçons suffisent, ce qui permet d'ordonner l'investigation secrète à un stade plus précoce de la procédure[1542]. A la lecture de l'art. 286 al. 1 let. a CPP, il reste néanmoins essentiel qu'une procédure pénale soit ouverte contre une personne déterminée, même si l'individu n'est pas encore identifié[1543]. Cette exigence permet d'éviter la recherche de preuves au hasard, comme cela avait court sous l'empire de l'aLFIS[1544].

b) La justification de la mesure au regard de la gravité de l'infraction

2006 En vertu de l'art. 286 al. 1 let. b CPP, une investigation secrète ne peut être mise en œuvre que si cette mesure se justifie au regard de la gravité de l'infraction.

2007 Cette condition part du postulat que malgré l'édiction d'un catalogue d'infractions, il faut vérifier concrètement si la gravité conditionnant la mise en œuvre de l'investigation secrète est suffisante[1545].

[1540] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 278; StPO-HANSJAKOB, art. 286 N 9.

[1541] BSK-StPO-KNODEL, art. 286 N 23; CR-CPP-JEANNERET, RYSER, art. 286 N 9; Message, CPP, p. 1238; SCHMID, Praxiskommentar, art. 286 N 6 ss.

[1542] BSK-StPO-KNODEL, art. 286 N 14; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 509.

[1543] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 278; Message, CPP, p. 1238; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 509.

[1544] ATF 134 IV 266, 275-276 = JdT 2008 IV 35, 50-51; TF 6B_211/2009 du 22 juin 2009, c. 1.2; BSK-StPO-KNODEL, art. 286 N 16; Message, CPP, p. 1238.

[1545] BSK-StPO-KNODEL, art. 286 N 20; PIETH, p. 152.

c) La subsidiarité de la mesure

2008 L'art. 286 al. 1 let. c CPP dispose qu'un autre acte d'instruction accompli jusqu'alors n'a pas abouti ou que les recherches sont sans issue ou excessivement difficiles sans le recours à l'investigation secrète.

2009 La concrétisation du principe de subsidiarité figurant à l'art. 197 al. 1 let. c CPP s'appréhende de manière similaire à celle, notamment, de l'art. 269 al. 1 let. c CPP[1546].

4. Les conditions formelles

a) La procédure d'autorisation

2010 La mise en œuvre d'une investigation secrète est soumise à l'autorisation d'une autorité judiciaire (art. 289 al. 1 CPP).

2011 Corrélativement à la procédure d'autorisation de la surveillance de la correspondance par poste et télécommunication, le ministère public doit – dans les vingt-quatre heures dès l'ordre d'infiltration[1547] – transmettre une demande au tribunal des mesures de contrainte qui statue dans les cinq jours (art. 289 al. 2 et 3 CPP). Si elle est accordée, l'autorisation est valable pour un an au plus et prolongeable par période de six mois au plus (art. 289 al. 5 CPP).

2012 Quant au contenu, la demande transmise au tribunal des mesures de contrainte doit exposer les motifs justifiant l'ordre d'investigation secrète. Ainsi, les faits présumés, les circonstances fondant les soupçons, les raisons pour lesquelles le principe de subsidiarité est rempli et la démonstration de la proportionnalité de l'usage de la mesure de contrainte doivent être explicités[1548]. En outre, le ministère public doit se prononcer sur la dotation d'identité secrète, la garantie de l'anonymat et sur la qualité des agents infiltrés[1549].

2013 Concernant l'autorisation, dans sa décision, le tribunal des mesures de contrainte se prononce sur la demande du ministère public en motivant sommairement sa décision et sur l'établissement des titres ou documents devant être établis pour l'identité d'emprunt, la garantie de l'anonymat et le recours à des agents infiltrés non-issus du corps de police (art.

[1546] Supra Partie II, Chapitre 3, I, A, 2, c, ii, a), 3, n° 1154 ss.

[1547] BSK-StPO-KNODEL, art. 289 N 3; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 281; MUGGLI, p. 267; SCHMID, Praxiskommentar, art. 289 N 5.

[1548] CR-CPP-JEANNERET, RYSER, art. 289 N 4; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-WOLTER, p. 281.

[1549] BSK-StPO-KNODEL, art. 289 N 14; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 512 et 515.

289 al. 3 et 4 CPP). Relevons encore que le tribunal des mesures de contrainte peut, moyennant une motivation accrue: autoriser provisoirement l'investigation, demander un complément au dossier ou des éclaircissements, ou refuser l'autorisation (art. 289 al. 3 phr. 2 CPP)[1550].

b) Les constatations fortuites

2014 Lorsque l'agent infiltré apprend l'existence d'infractions ne figurant pas dans la décision du ministère public et/ou dans l'autorisation du tribunal des mesures de contrainte, une nouvelle décision doit être ordonnée et une nouvelle autorisation être obtenue (art. 296 CPP).

2015 Par conséquent, les constatations fortuites ne sont exploitables qu'à deux conditions: l'infraction qu'elles élucident relève de la liste des comportements punissables (art. 286 al. 2 CPP) et une autorisation aurait pu être délivrée si des soupçons suffisants avaient existé[1551].

5. Les limites

a) De la mission

2016 Avant le début de la mission, le ministère public instruit l'agent infiltré (art. 290 CPP), c'est-à-dire qu'il fournit toutes les indications qui sont nécessaires et qui délimitent l'investigation secrète.

2017 Si de nouvelles instructions sont nécessaires au cours de l'investigation secrète – sans qu'il soit question de prolongation –, elles sont transmises à l'agent par le biais exclusivement de la personne de contact (art. 291 al. 1 CPP). Cette personne est un membre d'un corps de police qui instruit l'agent infiltré, le dirige et l'encadre (art. 287 al. 2 CPP *cum* art. 291 CPP). En d'autres termes, la personne de contact est le lien entre l'agent infiltré, le ministère public et les forces de police engagées.

2018 En vertu de l'art. 292 CPP, l'agent infiltré doit rendre compte à la personne de contact de manière complète et doit accomplir sa mission en respectant les instructions. S'il dépasse les limites autorisées par le ministère public, il est punissable (art. 293 al. 4 CPP). En revanche, lorsque l'agent infiltré dépasse inconsciemment ces limites suite à une transmission erronée

[1550] BSK-StPO-KNODEL, art. 289 N 14; HANSJAKOB, BÜPF/VÜPF, art. 7 N 19.

[1551] Supra Partie II, Chapitre 3, I, A, 2, c, v, d), n° 1215 ss.

des instructions par la personne de contact, il faut en conclure qu'il agit comme un instrument humain et que, par conséquent, seul l'auteur médiat – la personne de contact – est punissable[1552].

2019 Relevons au surplus qu'un agent infiltré ne doit pas inciter autrui à commettre une infraction. Notamment, dans le cadre de la surveillance sur Internet, il n'est pas autorisé à motiver la personne à passer à l'acte. Il peut en revanche tout à fait manifester son intérêt à – par exemple – obtenir des photos montrant des actes pédopornographiques[1553].

b) Le sort des preuves

2020 L'art. 289 al. 6 CPP règle la conséquence juridique lorsqu'une autorisation est refusée, qu'une autorisation provisoire est retirée, que la prolongation est refusée ou qu'aucune autorisation ou prolongation n'a été demandée.

2021 Dans ces hypothèses, tous les documents et enregistrements établis doivent être immédiatement détruits. Ils ne peuvent en aucun cas être utilisés comme moyen de preuve[1554]. Précisions toutefois que, concernant un refus de prolongation, seuls les documents ou enregistrements établis durant la mission non-autorisée sont soumis à la destruction immédiate[1555].

2022 La non-exploitabilité absolue est également de rigueur quand un agent provocateur a obtenu les preuves de manière illicite[1556].

2023 La situation est en revanche différente si l'agent infiltré réunit des preuves en sortant du cadre posé par sa mission. En effet, les art. 285a et ss CPP ne règlent pas cette problématique. Il faut donc se référer aux dispositions générales et conclure à l'applicabilité de l'art. 141 al. 2 CPP. Dès lors, l'exploitabilité des preuves recueillies dépend de leur nécessité pour élucider une infraction grave.

2024 Cette distinction entre l'exploitabilité des preuves obtenues par un agent infiltré de bonne foi mais dont la mission ne serait pas autorisée et celles obtenues de mauvaise foi par un agent

[1552] CONTAT, MÜLLER, p. 327-328.

[1553] CR-CPP-MOREILLON, MAZOU, art. 293 N 5; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 522-523.

[1554] BSK-StPO-KNODEL, art. 289 N 26; SCHMID, Praxiskommentar, art. 289 N 17.

[1555] HANSJAKOB, BÜPF/VÜPF, art. 7 N 46; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 515.

[1556] BSK-StPO-KNODEL, art. 293 N 13; HANSJAKOB, BÜPF/VÜPF, art. 7 N 37; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 515; SCHMID, Praxiskommentar, art. 289 N 7.

infiltré qui dépasse les limites autorisées est choquante. C'est pourquoi, afin de ne pas inciter les agents infiltrés à dépasser les instructions données, il serait plus logique de détruire également immédiatement les preuves recueillies et ne pas appliquer l'art. 141 al. 2 CPP.

6. La fin de l'investigation secrète

2025 Au sens de l'art. 289 al. 6 CPP, en cas d'absence d'autorisation ou de prolongement d'une investigation secrète, le ministère public est tenu de mettre fin sans délai à la mission secrète.

2026 En outre, à quelques nuances ou spécificités près, les conditions occasionnant la fin de la mesure et la communication au prévenu sont similaires à ce qui prévaut pour la surveillance de la correspondance par poste et télécommunication[1557]. Nous nous limitons donc ici aux spécificités de l'art. 297 al. 1 let. c et al. 3 CPP.

2027 Selon l'art. 297 al. 1 let. c CPP, la mission est immédiatement interrompue lorsque l'agent infiltré ou la personne de contact ne respecte pas les instructions du ministère public. Chaque manquement ne conduit pas à une interruption de la mission. En effet, seuls ceux rendant l'investigation secrète inutile, inefficace, dangereuse ou contraire au droit causent l'arrêt de l'activité de l'agent infiltré[1558].

2028 Quant à l'art. 297 al. 3 CPP, il est prévu que peu importe les circonstances ayant mené à la fin de l'investigation secrète[1559], l'autorité de poursuite pénale veille à ce qu'aucune personne ne soit exposée inutilement à des dangers.

c) Les recherches secrètes

1. La modification du Code de procédure pénale suisse entrée en vigueur le 1er mai 2013

2029 Originellement, le Code de procédure pénale suisse ne comprenait aucune disposition sur les recherches secrètes.

[1557] Supra Partie II, Chapitre 3, I, A, 2, c, iii, d) et e), n° 1191 ss et 1197 ss.

[1558] BSK-StPO-KNODEL, art. 297 N 6-7; Message, LSCPT, p. 3741; Polizeiliche Ermittlung-RHYNER, STÜSSI, p. 527-528; SCHMID, Praxiskommentar, art. 297 N 5-6.

[1559] Message, LSCPT, p. 3741.

2030 En date du 10 septembre 2012[1560], le Conseil national a adopté une révision du Code de procédure pénale suisse faisant suite à l'initiative parlementaire de Daniel Jositsch préconisant de restreindre le champ d'application de l'investigation secrète et d'autoriser les recherches secrètes.

2031 En revanche, dans la même initiative, la chambre du peuple à refuser de régler la question de l'investigation ou des recherches secrètes préventives estimant qu'il s'agissait d'une compétence purement cantonale que le fédéral ne peut pas réglementer[1561].

2032 L'initiative parlementaire fait suite à l'arrêt du Tribunal fédéral concernant une surveillance menée par la police zurichoise sur Internet[1562]. A l'aide du pseudonyme "Manuela_13", un agent est entré en contact avec un homme de 26 ans qui pensait s'entretenir avec une jeune fille de 13 ans. Après avoir orienté la conversation vers des sujets à caractère sexuel, l'homme a convenu un rendez-vous avec sa fausse interlocutrice. Le Tribunal fédéral a déclaré que toute prise de contact active par un policier qui agit secrètement et un interlocuteur doit être qualifiée d'investigation secrète[1563]. Dès lors, si aucune autorisation d'une autorité judiciaire indépendante n'a été donnée, il faut considérer la mesure policière comme illégale et, par conséquent, les preuves ne peuvent pas être exploitées[1564].

2033 Pour Daniel Jositsch et Franziska Mulle[1565], la décision du Tribunal fédéral a eu pour conséquence de restreindre considérablement le travail de la police, cette dernière ne pouvant en effet plus intervenir activement de manière spontanée sous une fausse identité, ni opérer des achats à des fins d'enquête.

2034 La révision du CPP proposée et entrée en vigueur le 1er mai 2013. Cette modification a permis, nous l'avons vu[1566], en premier lieu de définir plus strictement l'investigation secrète (art. 285a CPP) et de créer une base légale pour les recherches secrètes (art. 298a à 298d CPP).

[1560] Bulletin-officiel – Procès-verbaux du Conseil national du 10 septembre 2012 concernant l'initiative parlementaire: Investigation secrète – Restreindre le champ d'application des dispositions; BSK-StPO-KNODEL, art. 298a N 1.

[1561] ATF 140 I 381; RUDAZ, n° 51.

[1562] ATF 134 IV 266 = JdT 2008 IV 35.

[1563] ATF 134 IV 266, 274-278 = JdT 2008 IV 35, 47-52; StPO-HANSJAKOB, art. 298a N 4.

[1564] ATF 134 IV 266, 286-287 = JdT 2008 IV 35, 60-61.

[1565] JOSITCH, MULLE, p. 492.

[1566] Supra Partie II, Chapitre 3, III, A, 3, c, b), n° 1985 ss.

2. Les recherches secrètes

a) Le champ d'application

2035 La restriction du champ d'application de l'investigation secrète à l'art. 285a CPP – demandant une certaine durée de la mesure – a créé un vide juridique. C'est pourquoi le législateur a prévu l'introduction d'une nouvelle mesure: les recherches secrètes.

2036 En vertu de l'art. 298a al. 1 CPP: "les recherches secrètes consistent, pour les membres d'un corps de police, à tenter d'élucider des crimes ou des délits dans le cadre d'interventions de courte durée où leur identité et leur fonction ne sont pas reconnaissables, notamment en concluant des transactions fictives ou en donnant l'illusion de vouloir conclure de telles transactions.".

2037 A la différence des agents infiltrés, les agents affectés aux recherches secrètes ne sont pas munis d'une identité d'emprunt et leur activité est de courte durée (art. 298a al. 2 CPP)[1567].

2038 S'agissant de l'identité d'emprunt, il sied de préciser que rien n'empêche en revanche l'agent infiltré de se présenter sous un faux nom et une fausse adresse e-mail[1568]. En revanche, l'identité réelle de l'agent affecté figure dans les dossiers de procédure et peut être énoncé en audience[1569].

2039 A la lecture de la loi, les recherches secrètes sont donc une mesure se situant entre l'observation et l'investigation secrète[1570].

b) Les conditions matérielles et formelles

2040 Comme l'observation, les recherches secrètes sont ordonnées par la police pendant l'investigation policière ou par le ministère public après l'ouverture de l'instruction (art 298b

[1567]BSK-StPO-KNODEL, art. 298a N 2, 4-6 et et 9-10; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 243; EICKER, HUBER, p. 191; JOSITSCH, Strafprozessrechts, p.155; SCHMID, Handbuch, p. 533; SCHMID, Praxiskommentar, art. 298a N 1, 6, 9 et 13; StPO-HANSJAKOB, art. 298a N 1-2 et 14.

[1568] StPO-HANSJAKOB, art. 298a N 15.

[1569] BSK-StPO-KNODEL, art. 298a N 5-6 et 11-12; SCHMID, Handbuch, p. 533; SCHMID, Praxiskommentar, art. 298a N 15; StPO-HANSJAKOB, art. 298a N 17.

[1570] SCHMID, Praxiskommentar, art. 298a N 1-2; StPO-HANSJAKOB, art. 298a N 1.

al. 1 CPP)[1571]. Cette dernière doit recueillir l'autorisation du ministère public si la mesure se poursuit au-delà d'un mois (art. 298b al. 2 CPP).

2041 En outre, l'art. 298b CPP prévoit les conditions pour ordonner une telle mesure de contraintes qui sont similaires à ce qui prévaut pour l'observation (art. 282 CPP) à la différence près que des soupçons – et non des indices concrets – sont demandés[1572].

2042 En revanche, à la différence d'une simple observation, les recherches secrètes impliquent un comportement actif de l'agent[1573].

2043 Ce moyen de contrainte s'approche, sur ce point, de l'investigation secrète par la nature active des agissements de l'agent et par la qualité requise de l'agent, soit qu'il appartienne au corps de police (art. 298c CPP).

2044 Cela étant, à la différence de l'investigation secrète, une personne engagée à titre provisoire (art. 287 al. 1 let. b CPP) ne peut pas être affectée aux tâches de recherches secrètes, ceci s'explique par le fait qu'aucune autorité judiciaire ne contrôle l'ordre d'exécution de la mesure. En effet, pour le législateur, cette mesure de contrainte atteignant moins gravement aux droits fondamentaux que l'investigation secrète, l'autorisation d'un juge n'est pas nécessaire[1574].

2045 De même, contrairement aux mesures d'investigation secrète, les recherches secrètes sont de courte durée[1575]. Néanmoins, elles peuvent s'étendre dans le temps puisqu'une autorisation du ministère public est prévue au-delà d'un mois (art. 298b al. 2 CPP)[1576].

2046 En outre, les recherches secrètes ne sont pas limitées à certaines infractions. Elles peuvent se concevoir en relation avec n'importe quel crime ou délit (art. 298a al. 1 CPP)[1577].

[1571] BSK-StPO-KNODEL, art. 298b N 9; RIKLIN, art. 298b N 1; SCHMID, Praxiskommentar, art. 298b N 3; StPO-HANSJAKOB, art. 298b N 1.

[1572] BSK-StPO-KNODEL, art. 298b N 7; JOSITSCH, Strafprozessrechts, p. 155; SCHMID, Praxiskommentar, art. 298b N 3-4; StPO-HANSJAKOB, art. 298b N 2.

[1573] JOSITSCH, Strafprozessrechts, p. 155; SCHMID, Handbuch, p. 533; SCHMID, Praxiskommentar, art. 298a N 8; StPO-HANSJAKOB, art. 298a N 5.

[1574] BSK-StPO-KNODEL, art. 298c N 2; SCHMID, Handbuch, p. 536; SCHMID, Praxiskommentar, art. 298c N 1; StPO-HANSJAKOB, art. 298c N 1.

[1575] EICKER, HUBER, p. 191.

[1576] RIKLIN, art. 298b N 5; SCHMID, Handbuch, p. 535; SCHMID, Praxiskommentar, art. 298a N 5; StPO-HANSJAKOB, art. 298a N 8-9.

[1577] StPO-HANSJAKOB, art. 298a N 10.

2047 Pour finir, les recherches secrètes ne sont pas soumises à l'obligation d'une identité d'emprunt et ne garantissent pas l'anonymat des agents affectés à cette tâche (art. 298a al. 2 CPP).

2048 S'agissant de la fin des recherches secrètes et de la communication, l'art. 298d CPP est similaire à ce qui prévaut pour l'investigation secrète, extensivement à ce qui prévaut pour la surveillance de la correspondance par poste et télécommunication (art. 297 CPP)[1578]. Nous ne limiterons à renvoyer à notre commentaire à ce sujet, hormis pour préciser que, faute d'identité secrète, l'art. 298d al. 3 CPP prévoit que l'agent affecté ne soit pas exposé inutilement afin de le protéger et respecter sa liberté personnelle[1579].

2049 Relevons encore que les recherches secrètes comme l'observation qui demande des indices concrets et l'investigation qui est conditionnée à l'existence de soupçons, cette mesure ne peut être ordonnées que moyennant l'existence de soupçons, même vagues. Dès lors, les art. 298a à 298d CPP ne réglementent en aucun cas la surveillance préventive qui est du ressort des cantons[1580].

c) Les limites des nouvelles dispositions légales sur les recherches secrètes et l'investigation secrète

2050 L'instauration des recherches secrètes comme mesure de contrainte et des dispositions telles qu'édictées sont critiquables.

2051 Premièrement, le comportement prévu comme recherches secrètes est le plus fréquent dans le travail répressif au cours de l'investigation policière. Ainsi, l'investigation secrète risque de perdre toute son utilité alors même qu'elle offre – par ses conditions plus restrictives – une meilleure garantie du respect des droits fondamentaux.

2052 Deuxièmement, l'absence d'autorisation par le tribunal des mesures de contrainte porte préjudice aux droits élémentaires de la procédure. Normalement, toute mesure de contrainte est ordonnée par le ministère public et autorisée par une autorité judiciaire. Il semble que cette solution devrait avoir cours pour les recherches secrètes. En effet, il est à craindre qu'à défaut d'un régime d'autorisation, la police utilise les dispositions des art. 298a à 298d CPP

[1578] JOSITSCH, Strafprozessrechts, p. 157; RIKLIN, art. 298d N 1; SCHMID, Handbuch, p. 537; SCHMID, Praxiskommentar, art. 298d N 1 ss; StPO-HANSJAKOB, art. 298d N 1. Supra Partie II, Chapitre 3, I, A, 2, c, iii, d) et e), n° 1191 ss et 1197 ss.

[1579] BSK-StPO-KNODEL, art. 298d N 10; SCHMID, Handbuch, p. 537-538.

[1580] BSK-StPO-KNODEL, art. 298b N 6; RIKLIN, art. 298b N 3; RUDAZ, n° 51; StPO-HANSJAKOB, art. 298a N 11.

pour procéder à des mesures préventives, ce qui n'est en aucun cas autorisé par les articles précités[1581].

2053 Quant aux recherches secrètes concernant le cadre de notre étude, soit la surveillance sur Internet, elle ne nous semble pas réellement applicable. En effet, les recherches secrètes sont définies comme de courte durée, alors que la surveillance, notamment sur des groupes de discussion, est généralement étendue dans le temps.

2054 Si nous considérons que les recherches secrètes peuvent avoir une certaine durée, puisqu'une autorisation du ministère public est possible au-delà d'un mois, nous serons face à deux problématiques. Premièrement, le critère de distinction entre investigation secrète et recherches secrètes ne serait pas la durée, mais bel et bien la nécessité ou non d'une identité d'emprunt. Deuxièmement, la surveillance sur Internet ne demandant pas d'identité d'emprunt attestée par un acte authentique, les agents chargés de la cybercriminalité verraient systématiquement leur identité dévoilée (art. 298a al. 2 CPP), ce qui peut largement nuire à la bonne administration de la justice.

ii. En cas de surveillance de l'accès Internet

2055 L'anonymisation sur Internet avec la pseudonymisation des usagers complique la tâche de l'autorité pénale. L'évolution du Peer-to-Peer, du téléchargement illégal et de la criminalité effectuée sous le couvert d'un pseudonyme ou d'un nom d'emprunt ont forcé les autorités à recourir à la preuve par IP et/ou à la preuve par adresse MAC.

2056 En droit suisse, l'adresse IP (art. 24*b* let. b ch. 3 OSCPT) et l'adresse MAC (art. 24*a* let. b ch. 5 et 24*b* let. a ch. 5 OSCPT) sont des données de télécommunication qui peuvent être fournies lors d'une surveillance de l'envoi ou de la réception de messages par le biais d'un service de messagerie électronique asynchrone, respectivement en cas de surveillance de l'accès Internet. Lors de l'analyse des mesures de surveillance des télécommunications, nous avons exposé la procédure des art. 269 ss CPP[1582]. Les principes et conditions exposées à l'aune de cette surveillance valent *mutatis mutandis*, avec la précision que si l'infraction a été réalisée au moyen d'Internet, l'art. 14 al. 4 LSCPT s'applique et, par voie de conséquence, aucune limitation de temps pour la collecte des données rétroactive n'existe[1583].

[1581] Initiative parlementaire 08.458 – Synthèse des résultats, p. 15.

[1582] Supra Partie II, Chapitre 3, I, A, 2, c, n° 1142 ss.

[1583] ATF 139 IV 98, 101-102 = JdT 2014 IV 3, 6-7.

2057 En outre, l'art. 27 al. 1 OSCPT prévoit que les fournisseurs d'accès Internet – ce qui exclut les exploitants de réseaux domestiques, les fournisseurs de messageries, blogs ou autres pages internet – sont soumis à l'obligation de fournir les renseignements sur les usagers d'Internet en cas de demande de l'autorité. Dans le cas d'une demande s'intéressant à l'adresse IP attribuée, le fournisseur doit transmettre: "*le type de raccordement, la date et l'heure de l'attribution ou la date et l'heure du début et le cas échéant de la fin de la période de l'attribution, le nom, l'adresse, les données utilisées pour la procédure d'identification (login) et, si elle est connue, la profession de l'usager ainsi que les autres adresses IP que le fournisseur d'accès à Internet lui a attribuées*" (art. 27 al. 1 let. a OSCPT).

2058 Les demandes de renseignements sont soumises à la même procédure que celle concernant la surveillance des données accessoires (art. 273 CPP)[1584], étant précisé que l'obtention des renseignements est subordonnée à la réalisation de conditions moins strictes que l'interception et l'enregistrement de la correspondance dès lors que l'atteinte aux droits fondamentaux est moins grave[1585].

iii. La perquisition des documents électroniques

2059 En ce qui concerne les fichiers, les emails et autres documents informatiques, les prescriptions des art. 269 ss CPP se rapportent uniquement aux données en voie de transmission[1586].

2060 A partir du moment où une donnée se trouve encore chez l'expéditeur, qu'elle est arrivée chez le destinataire ou qu'il s'agit d'un fichier enregistré sur un support de stockage qui n'est pas destiné à être envoyé, les dispositions relatives à la perquisition et au séquestre sont applicables (art. 241 ss et 263 ss CPP, en particulier art. 246-248 CPP)[1587].

2061 A noter qu'en ce qui concerne les données de localisation GPS, les historiques ou les données enregistrées sur un serveur sont également soumis aux dispositions sur la perquisition et le séquestre.

[1584] Supra Partie II, Chapitre 3, I, A, 2, c, n° 1142 ss.

[1585] Message, CPP, p. 1232.

[1586] ATF 140 IV 181, 187 = JdT 2015 IV 167, 172.

[1587] ATF 140 IV 181, 187 = JdT 2015 IV 167, 172; GLESS, p. 3 et 7; JEAN-RICHARD-DIT-BRESSEL, Mailbox, p. 159-160.

a) Le champ d'application

2062 La perquisition de documents et d'enregistrements permet de lire ou de regarder un fichier afin d'en connaître le contenu, de déterminer si les données sont susceptibles d'être utilisées comme preuve et, le cas échéant, si elles doivent être consignées au dossier[1588]; en d'autres termes, de mettre en sureté des moyens de preuves (art. 196 let. a CPP).

2063 Ce type de perquisition vise spécifiquement les documents physiques, les enregistrements audio, vidéo, les supports informatiques ainsi que les installations destinées au traitement et à l'enregistrement d'informations (art. 246 CPP)[1589].

2064 Concernant les données informatiques, la disposition ne limite ni la nature des données, ni le moyen de stockage. Ainsi, tout fichier – écrit, image, audio, vidéo, etc. – enregistré sur tout type de support informatique – disque dur interne, disque dur externe, clé USB, disquette, CD-ROM, mémoire vive interne, etc. – est susceptible d'être perquisitionné[1590].

b) L'ordre de perquisition

1. Compétence, forme et contenu de l'ordre de perquisition

2065 L'art. 198 al. 1 CPP détermine la compétence pour ordonner une mesure de contrainte (art. 196 CPP), notamment la perquisition de documents ou d'enregistrements contenus sur un support informatique.

2066 En règle générale, le ministère public après ouverture d'une instruction (art. 198 al. 1 let. a CPP *cum* 309 al. 1 let. b CPP) et, après l'inculpation, le tribunal ou la direction de la procédure en cas d'urgence (art. 198 al. 1 let. b CPP *cum* 328 CPP) sont habilités à ordonner la mesure[1591]. Pour ce faire, ils doivent délivrer un mandat écrit indiquant les documents à examiner, le but de la mesure et les autorités ou personnes chargées de l'exécuter (art. 241

[1588] ATF 109 IV 153, 154 = JdT 1984 IV 123; ATF 130 II 302, 304.

[1589] ATF 139 IV 128, 132-133 = JdT 2014 IV 15, 18-19; EICKER, HUBER, p. 171; MOREILLON, PAREIN-REYMOND, art. 246 N 3; RIEDO, FIOLKA, NIGGLI, p. 290.

[1590] ATF 108 IV 76; ATF 130 II 302, 304; BSK-StPO-THORMANN, BRECHBÜHL, art. 246 N 3; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 215-216; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 233; Message, CPP, p. 1220; MOREILLON, PAREIN-REYMOND, art. 246 N 1-3; Polizeiliche Ermittlung-ARMBRUSTER, p. 357; SCHMID, Handbuch, p. 461; SCHMID, Praxiskommentar, art. 246 N 1.

[1591] ATF 139 IV 128, 133 = JdT 2014 IV 15, 18.

al. 2 CPP *cum* 80 CPP). Toutefois, en cas d'urgence, un mandat oral – suivi d'une confirmation écrite – peut être délivré (art. 241 al. 1 CPP).

2067 En cas de péril en la demeure – par exemple, si le but visé par la perquisition est compromis dans l'intervalle –, la police est autorisée à exécuter la perquisition sans mandat en informant toutefois sans délai l'autorité pénale compétente – ministère public ou tribunal – (art. 198 al. 1 let. c *cum* art. 213 al. 2 et/ou 241 al. 3 CPP)[1592].

2. Les conditions à respecter pour la perquisition des documents et enregistrements

2068 Pour assurer la protection des informations sensibles ou secrètes, la lettre de l'art. 246 CPP subordonne la perquisition des documents et enregistrements à l'exigence que les informations contenues dans les documents ou les enregistrements puissent faire l'objet d'un séquestre.

2069 En vertu de l'art. 263 al. 1 let. a CPP, cette exigence est réalisée si les documents et enregistrements sont utilisés par la suite comme moyen de preuve. L'utilité doit s'apprécier sur la base d'indices concrets, en gardant à l'esprit qu'une utilité potentielle est suffisante[1593]. Dès lors, l'autorité pénale ne peut pas effectuer une perquisition à des fins exploratoires[1594], elle doit avoir suffisamment d'indices lui faisant penser que les fichiers informatiques – notamment – sont utiles à l'administration de la justice, sans quoi les preuves sont irrecevables et inexploitables[1595].

2070 Relevons encore que selon l'art. 264 CPP, les documents et enregistrements ne peuvent être séquestrés lorsqu'ils concernent la sphère privée du prévenu ou de tiers, ou qu'ils contiennent des secrets protégés par la loi.

2071 Ainsi, la correspondance entre le prévenu et son défenseur (art. 264 al. 1 let. a CPP), les documents personnels et la correspondance du prévenu si l'intérêt à la protection de la personnalité prime l'intérêt de la poursuite pénale (art. 264 al. 1 let. b CPP), les objets, notamment les documents et la correspondance qui proviennent de relations établies entre le

---

[1592] ATF 139 IV 128, 133-134 = JdT 2014 IV 15, 19-20; Message, CPP, p. 1219; SCHMID, Handbuch, p. 457.

[1593] ATF 119 IV 175, 178 = JdT 1995 IV 125; ATF 122 II 367, 371 = JdT 1998 IV 127, 127-128; ATF 130 II 193, 197-198 = JdT 2005 IV 309, 313; ATF 134 II 318, 327; ATF 136 IV 82, 85-86; BSK-StPO-THORMANN, BRECHBÜHL, art. 246 N 7; CR-CPP-CHIRAZI, art. 246 N 5; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 224; OBERHOLZER, Strafprozessrechts, p. 401.

[1594] ATF 103 Ia 206, 216-217 = JdT 1979 IV 16, 22-23; ATF 126 II 495, 505.

[1595] ATF 125 II 65, 73; ATF 129 IV 141, 145.

prévenu et une personne ayant le droit de refuser de témoigner en vertu des art. 170 à 173 CPP et qui n'a pas le statut de prévenu[1596], n'a pas agi au préjudice de son client, en connivence avec lui ou au détriment d'un tiers[1597] (art. 264 al. 1 let. c CPP) doivent être mis sous scellé suite à la demande de la personne qui entend s'opposer à la perquisition et au séquestre (art. 248 al. 1 et 264 al. 3 CPP)[1598].

c) L'exécution de la perquisition

2072 L'exécution de la perquisition des documents et enregistrements est prévue aux art. 242 et 247 CPP.

1. Les dispositions générales

2073 L'autorité ou la personne chargée d'exécuter la mesure – la police, le ministère public, le tribunal de première instance ou la juridiction d'appel (art. 12, 13 let. b et 2, 198 al. 2 CPP *cum* 242 al. 1 CPP) – doit mettre en œuvre tous les moyens aptes et nécessaires à la sauvegarde du but d'intérêt public que représente la perquisition, soit notamment de permettre le séquestre des moyens de preuves (art. 242 al. 1 CPP).

2074 Ainsi, lorsque l'autorité ou la personne chargée d'exécuter le mandat de perquisition agit, elle doit respecter le principe de proportionnalité, étant précisé que ce principe est explicitement prévu à l'art. 200 CPP qui dispose que le recours à la force – *in casu* à la perquisition de documents et d'enregistrements – ne peut être utilisé qu'en dernier recours.

2075 En outre, l'autorité compétente pour exécuter la mesure de contrainte doit communiquer le mandat à la personne directement touchée par la perquisition des documents lorsqu'elle est ordonnée par écrit (art. 199 CPP)[1599]. Si les informations obtenues par la perquisition concernent un tiers, une copie du mandat ne doit donc pas lui être remise[1600]. L'autorité compétente doit également fournir une copie d'un éventuel procès-verbal d'exécution.

[1596] ATF 102 Ia 516, 519-520 = JdT 1978 IV 128; ATF 102 IV 210, 214 = JdT 1977 IV 128; ATF 117 Ia 341, 350; ATF 125 I 46, 50 = JdT 2000 IV 17, 21; ATF 126 II 495, 505; ATF 127 II 151, 154; ATF 130 II 193, 195-196 = JdT 2005 IV 309, 311-312.

[1597] ATF 102 IV 210, 214 = JdT 1977 IV 128.

[1598] Infra Partie II, Chapitre 3, III, A, 3, c, iii, d), 2, n° 2083-2084.

[1599] BSK-StPO-THORMANN, BRECHBÜHL, art. 246 N 5; EICKER, HUBER, p. 178; SCHMID, Handbuch, p. 453-454.

[1600] CR-CPP-VIREDAZ, JOHNER, art. 199 N 2; SCHMID, Praxiskommentar, art. 199 N 1.

2. Les dispositions spéciales

2076 La perquisition des documents et des enregistrements doit être exécutée en respectant au maximum la confidentialité[1601], notamment en respectant le secret professionnel et en évitant que des informations non nécessaires à l'affaire soient recueillies[1602]. C'est pourquoi le détenteur effectif des documents et enregistrements a le droit de se déterminer préalablement sur leur contenu, et ainsi éventuellement demander que leur lecture ne soit pas réalisée (art. 247 al. 1 CPP)[1603].

2077 A l'introduction du Code de procédure pénale suisse, une controverse existait quant à savoir si l'ayant droit des données pouvait également s'opposer à la perquisition et au séquestre. Dans un arrêt récent[1604], le Tribunal fédéral a tranché cette question. La Haute cour a mis en lien l'art. 248 CPP et l'art. 264 CPP concluant qu'autant le détenteur effectif des données que l'ayant droit du secret peut requérir la mise sous scellé des informations recueillies à la suite d'une perquisition dès qu'il a connaissance de cette mesure[1605].

2078 Avant la perquisition des documents ou enregistrements, le détenteur peut faire usage de son droit – droit qui devra d'emblée être signalé[1606] – et avertir l'autorité qu'il s'agit d'informations qui ne peuvent servir de preuves ou qui sont couvertes par un secret privé ou professionnel (art. 246 *cum* 264 CPP)[1607]. Néanmoins, un examen sommaire – soit un rapide coup d'œil – par l'autorité pénale est inévitable pour se déterminer sur le sort à réserver à la pièce[1608]. L'ayant droit bénéficie du même droit.

2079 Dans la pratique, le tri des données électroniques sur place est particulièrement délicat. Afin d'éviter qu'elles soient modifiées, elles sont généralement copiées sur un support

[1601] BSK-StPO-THORMANN, BRECHBÜHL, art. 248 N 2; PIQUEREZ, Traité de procédure pénale suisse, p. 586; Polizeiliche Ermittlung-ARMBRUSTER, p. 358; SCHMID, Handbuch, p. 463-464.

[1602] ATF 141 IV 77, 82-86; ATF 138 IV 225, 228 = JdT 2014 IV 24, 26.

[1603] ATF 127 II 151, 155-157; ATF 140 IV 28, 37 = JdT 2014 IV 206, 214; BSK-StPO-THORMANN, BRECHBÜHL, art. 247 N 3; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 216; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 234; Polizeiliche Ermittlung-ARMBRUSTER, p. 354; SCHMID, Praxiskommentar, art. 247 N 1.

[1604] ATF 140 IV 28, 34-38 = JdT 2014 IV 206, 212-216

[1605] ATF 140 IV 28, 37 = JdT 2014 IV 206, 214

[1606] TF 1B_320/2012, c. 4.5 = SJ 2013 I 333; BSK-StPO-THORMANN, BRECHBÜHL, art. 247 N 3-4; CR-CPP-CHIRAZI, art. 247 N 3; StPO-KELLER, art. 247 N 1.

[1607] GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 234; SCHMID, Praxiskommentar, art. 247 N 3.

[1608] ATF 106 IV 413, 423-425 = JdT 1982 IV 124, 125-127; ATF 108 IV 76; TPF 2005 190, c. 4.3; BE.2011.6, c. 1.3; CR-CPP-CHIRAZI, art. 247 N 6; DONATSCH, SCHWARZENEGGER, WOHLERS, p. 216; PERRIER DEPEURSINGE, art. 248, p. 320; HAUSER, SCHWERI, HARTMANN, p. 352; OBERHOLZER, Strafprozessrechts, p. 388; Polizeiliche Ermittlung-ARMBRUSTER, p. 358.

informatique. Les supports de données sont alors extraits et renvoyés au moyen d'un Software – logiciel de traitement – spécifique. Toutes les données – même celles cachées, cryptées, protégées par un mot de passe ou effacées – sont alors copiées. Ainsi, les lacunes existantes dans le tri des informations électroniques impliquent que des informations sans aucune importance probatoire sont séquestrées[1609].

2080 Afin que le tri des documents soit réalisé de manière efficace et dans le respect de la confidentialité, qu'il soit fait sur place ou, comme pour le matériel informatique, dans d'autres locaux, le recours à un expert externe est possible (art. 247 al. 2 CPP *cum* 182 ss CPP)[1610]. Le rôle de l'expert est alors d'examiner le contenu des documents et enregistrements afin de déterminer s'ils sont ou non pertinents et/ou protégés par un secret.

2081 Relevons encore que, dans le respect du principe de proportionnalité, le détenteur peut remettre des copies des documents et enregistrements ou un tirage de ceux-ci si cela suffit aux besoins de la procédure (art. 247 al. 3 CPP). Sous la menace de sanction (art. 292 CP), pour autant que le détenteur ne soit pas le prévenu ou une personne bénéficiant du droit de refuser de témoigner (art. 265 al. 2 CPP), il peut même être astreint à remettre des copies sous forme papier ou sous forme de support de données[1611].

d) Les données recueillies

1. Les données informatiques utiles

2082 Nous l'avons énoncé[1612], la perquisition vise à acquérir des preuves documentaires afin d'élucider les faits, et/ou d'identifier l'auteur et/ou les participants.

2083 Ainsi, certains documents et enregistrements sont utiles à l'enquête et peuvent s'avérer être des moyens de preuves pertinents. Tous ces éléments, étant susceptibles de servir à la

[1609] Polizeiliche Ermittlung-ARMBRUSTER, p. 358-359.

[1610] BSK-StPO-THORMANN, BRECHBÜHL, art. 247 N 19; JEANNERET, KÜHN, p. 272; Message, CPP, p. 1220. Supra Partie II, Chapitre 1, n° 385 ss.

[1611] CourEDH, Affaire *Saunders c. Royaume-Uni*, arrêt du 17 décembre 1996, § 68-69; CourEDH, Affaire *J.B. c. Suisse*, arrêt du 3 mai 2001, 31827/96, § 64; CourEDH, Affaire *Jalloh c. Allemagne*, arrêt du 11 juillet 2006, 54810/00, § 100; CourEDH, Affaire *Kolu c. Turquie*, arrêt du 2 août 2005, 35811/97, § 51; CourEDH, Affaire *O'Halloran et Francis c. Royaume-Uni*, arrêt du 29 juin 2007, 15809/02 et 25624/02, § 53-63; CourEDH, Affaire *Brusco c. France*, arrêt du 14 octobre 2010, 1466/07, § 44; BSK-StPO-THORMANN, BRECHBÜHL, art. 247 N 33 ; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 235; Message, CPP, p. 1220; SCHMID, Handbuch, p. 461-462.

[1612] Supra Partie II, Chapitre 3, III, A, 3, iii, n° 2059 ss.

manifestation de la vérité au cours du procès pénal, sont mis en sûreté afin de garantir leur protection et leur conservation (art. 263 ss CPP).

2. La mise sous scellé

2084 Si un titulaire de documents ou d'enregistrements s'oppose à la perquisition et au séquestre au motif qu'il est couvert par un secret privé ou professionnel ou pour d'autres motifs – informations non pertinentes à l'affaire en cause – et que l'autorité persiste à vouloir saisir les documents et enregistrements, le détenteur et/ou l'ayant droit peuvent demander la mise sous scellé (art. 248 al. 1 CPP). Ce droit appartient au prévenu ou aux tiers et permet de s'opposer tant à la perquisition qu'à un ordre de production[1613].

2085 Pour obtenir la mise sous scellé, le détenteur doit immédiatement ou l'ayant droit dès qu'il a connaissance de la perquisition et du séquestre – avant le commencement de l'évaluation des informations – en formuler la demande et rendre vraisemblable que son droit de refuser de témoigner, de déposer ou d'autres motifs existent[1614].

2086 Dans un tel cas, la perquisition est paralysée. Les autorités d'instruction sont obligées de procéder à la mise sous scellé et, par conséquent, n'ont pas le droit de consulter et d'exploiter les documents ou enregistrements concernés (art. 248 al. 1 *in fine* CPP), exception faite de la réalisation d'un examen sommaire[1615].

2087 L'autorité pénale qui considère que les documents et enregistrements placés sous scellés sont utiles à l'enquête et ne sont pas protégés par un secret professionnel ou un intérêt privé prépondérant peut demander la levée des scellés (art. 248 al. 2 CPP).

[1613] ATF 121 I 240; ATF 140 IV 28, 35-36; BSK-StPO-THORMANN, BRECHBÜHL, art. 248 N 1-2; HAUSER, SCHWERI, HARTMANN, p. 353; OBERHOLZER, Strafprozessrechts, p. 387; SCHMID, Handbuch, p. 463-464; SCHMID, Praxiskommentar, art. 248 N 3.

[1614] ATF 114 Ib 357, 360-361 = JdT 1990 IV 60, 61; ATF 127 II 151, 155-156; TF 1B_477/2012 du 13 février 2013, c. 3.2; TF 1B_516/2012 du 9 janvier 2013, c. 2 BSK-StPO-THORMANN, BRECHBÜHL, art. 248 N 9; Message, CPP, p. 1221;.PERRIER DEPEURSINGE, art. 248, p. 320; Polizeiliche Ermittlung-ARMBRUSTER, p. 361

[1615] ATF 106 IV 413, 423 = JdT 1982 IV 124, 126-127; ATF 108 IV 76; TPF 2005 190, c. 4.3; BE.2011.6, c. 1.3; BSK-StPO-THORMANN, BRECHBÜHL, art. 248 N 13; GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-LIPS-AMSLER, p. 236; OBERHOLZER, Strafprozessrechts, p. 388; SCHMID, Handbuch, p. 463-464. Supra Partie II, Chapitre 3, III, A, 3, c, iii, c), n° 2076.

2088 Sous peine de péremption et de restitution des documents et enregistrement au détenteur, la demande de levée des scellés doit s'effectuer dans les vingt jours à compter de la requête de mise sous scellé (art. 248 al. 2 CPP *cum* art. 89 al. 1 CPP)[1616].

2089 Dans le cadre de la procédure préliminaire, il appartient au juge du tribunal des mesures de contrainte de déterminer, dans le mois qui suit le dépôt de la demande, si les conditions de la perquisition sont remplies et si la mise sous scellé est fondée. Pour ce faire, il réalise une pesée des intérêts entre l'intérêt à la poursuite et l'intérêt à la confidentialité des données (art. 248 al. 3 let. a CPP)[1617]. Dans les autres cas, le tribunal saisi de la cause est compétent pour trancher la question (art. 248 al. 3 let. b CPP).

2090 Relevons que le délai d'un mois pour se prononcer est un simple délai d'ordre. Dans le cadre de dossier contenant un nombre certain de documents et d'enregistrements ou si l'avis d'un expert est requis (art. 248 al. 4 CPP *cum* 182 ss CPP), le délai peut être prolongé tant qu'il ne paralyse pas de manière disproportionnée la procédure[1618].

2091 Par conséquent, lorsqu'une demande de mise sous scellé est effectuée, plusieurs cas de figure existent quant à l'exploitabilité des données:

- si l'autorité pénale ne demande pas la levée dans les vingt jours, les documents et enregistrements sont inexploitables;
- si une demande de levée est transmise au tribunal compétent, celui-ci statue définitivement (art. 380 et 393 ss CPP). La levée des scellés rend consultable les documents et enregistrements, conséquemment ils peuvent être administrés comme preuve, alors que le refus de la levée des scellés confirme l'interdiction d'exploiter les documents.

3. Les découvertes fortuites

2092 Comme toutes mesures de contrainte, la perquisition des documents et enregistrements ne peut être ordonnée que sur la base de soupçons suffisants se rapportant à une infraction déterminée (art. 197 al. 1 let. b CPP). Néanmoins, à l'occasion de l'exécution de la

[1616] ATF 139 IV 246, 249-250; JdT 2014 IV 85, 87-88; BSK-StPO-THORMANN, BRECHBÜHL, art. 248 N 18; PERRIER DEPEURSINGE, art. 248, p. 320; SCHMID, Handbuch, p. 463-464; SCHMID, Praxiskommentar, art. 248 N 8.

[1617] ATF 122 IV 91, 96; ATF 125 IV 222, c. 2; ATF 137 IV 189, 195-196 = JdT 2012 IV 90; BV.2005.15, c. 3.1; BE.2006.6, c. 3; BV.2010.11, c. 3.3; SCHMID, Praxiskommentar, art. 248 N 11-12.

[1618] JEANNERET, KÜHN, p. 272; Message, CPP, p. 1221; PERRIER DEPEURSINGE, art. 248, p. 322.

perquisition, il se peut que l'autorité pénale découvre des indices laissant présumer la commission d'une autre infraction.

2093 En cas de découvertes fortuites, l'art. 243 CPP prévoit que les documents ou enregistrements qui concernent cette autre infraction doivent être mis en sûreté et transmis immédiatement à la direction de la procédure. Cette dernière décide de la suite de la procédure, notamment de savoir si les découvertes fortuites sont exploitables[1619].

2094 L'art. 243 CPP, contrairement à l'art. 278 CPP, est muet concernant les critères que l'autorité doit prendre en considération pour sa décision. Selon la jurisprudence et la doctrine, toute découverte fortuite est exploitable si les conditions légales posées à son obtention sont réalisées en vertu d'un contrôle subséquent[1620]. Dans le cas contraire, l'exploitation des découvertes fortuites n'est envisageable que pour élucider une infraction grave qui ne pourrait être élucidée sans cette découverte (art. 141 al. 2 CPP).

2095 Il nous faut préciser que si les découvertes fortuites concernent un secret protégé de manière absolue, l'élément probatoire n'est pas exploitable (art. 271 al. 2 CPP *par analogie*). Une pesée des intérêts devra en outre avoir lieu si la preuve relève de la sphère privée de leur détenteur et contient donc des secrets privés. En cas de litige sur la qualité des découvertes fortuites, le détenteur et/ou l'ayant droit doivent demander la mise sous scellé (art. 248 CPP).

4. L'efficacité et l'utilisation comme preuve des données informatiques

2096 Dans un objectif d'efficacité de la poursuite et de la répression pénale, les indices informatiques constituent un outil essentiel. En effet, la recherche d'éléments, de documents, d'enregistrements ou de traces peut conduire à la constitution de faisceaux d'indices susceptibles de servir d'éléments probatoires.

a. L'utilité de la surveillance sur Internet et les moyens de preuves issus de cette surveillance

2097 La surveillance sur Internet offre à l'autorité pénale un vaste choix de techniques et d'interception de données.

[1619] ATF 139 IV 128, 135-137 = JdT 2014 IV 15, 22-23; JEANNERET, KÜHN, p. 267.

[1620] CR-CPP-CHIRAZI, art. 243 N 8; HAUSER, SCHWERI, HARTMANN, p. 352; Polizeiliche Ermittlung-ARMBRUSTER, p. 352.

2098 Dans le monde actuel, le cyberespace est employé quotidiennement par de nombreuses personnes. Grâce au réseau Internet, il est possible de communiquer rapidement, d'échanger des idées ou des points de vues avec des personnes tierces inconnues, d'obtenir des conseils de ces mêmes personnes ou encore de trouver des informations, des avis ou des recommandations sur des domaines spécifiques fournis par des amateurs, des professionnels ou des spécialistes.

2099 Ces diverses possibilités ont facilité la tâche des délinquants professionnels et amateurs. En effet, il est devenu plus facile pour eux d'échanger avec des complices et des coauteurs ou même d'instiguer des inconnus, de se procurer les informations et les outils nécessaires pour commettre leur infraction, ou encore de découvrir dans toutes les données émises, transmises et disponibles sur le net l'objet de leur infraction, notamment des photos à caractère pornographique et/ou pédopornographie. Ce ne sont là que quelques exemples des possibilités d'Internet.

2100 Pour éviter que le réseau d'échange mondial ne soit un univers où les délinquants restent impunis et pour découvrir, élucider ou constituer des éléments de preuve, l'autorité pénale a diverses ressources qui lui permettent de recueillir des éléments servant à la découverte de la vérité matérielle et/ou d'identifier les auteurs.

2101 Il est impossible d'être exhaustif quant aux possibilités qu'offre Internet pour l'enquête policière et la procédure pénale. Néanmoins, quelques techniques d'investigation méritent que nous y fassions référence.

2102 Concernant le Peer-to-Peer, certains logiciels offrent immédiatement la possibilité de connaître l'adresse IP d'un utilisateur, plus exactement d'un uploader. Par exemple, lorsque nous téléchargeons un fichier à l'aide du logiciel emule, il est possible de cliquer sur le téléchargement et d'obtenir la liste des sources avec pseudonyme et adresse IP. Les deux premiers chiffres permettant d'identifier le pays et la ville, l'autorité compétente peut cibler certains fichiers à caractère pornographique – par exemple – et découvrir si une source en Suisse le transmet. Une fois l'adresse obtenue, une enquête peut être diligentée et le renseignement auprès du fournisseur d'accès Internet permet d'obtenir l'identité réelle de l'utilisateur. Notons qu'il s'agit généralement d'une mesure préventive qui doit être prévue par une norme cantonale.

2103 Une autre possibilité qui concerne également l'identification des utilisateurs soit de service Peer-to-Peer, soit de groupes de discussion ou de services sociaux est l'utilisation de logiciel qui trace l'adresse IP. Ce type de programme permet uniquement d'obtenir l'adresse IP, voire de géolocaliser globalement le lieu de connexion de l'utilisateur. En revanche, la connexion à

Internet passant par des routeurs et des répartiteurs appartenant aux fournisseurs d'accès Internet, l'aide de ce dernier pour identifier l'utilisateur reste nécessaire ce d'autant que les adresses IP sont généralement dynamiques.

2104 Outre l'identification pure des usagers, la surveillance sur Internet est utile pour obtenir des données, des renseignements ou plus spécifiquement des indices servant soit à identifier l'auteur d'une infraction et/ou l'interlocuteur, soit d'élucider le déroulement d'un acte délictuel, voire de prévenir un tel acte. La récolte de ces éléments probatoires est réalisée soit directement, c'est-à-dire suite à un échange avec un interlocuteur par exemple, soit indirectement en introduisant par exemple un cheval de Troie dans l'ordinateur d'un suspect afin d'acquérir les données qui transitent par Internet. Précisons que ce ne sont que des exemples et que d'autres méthodes directes ou indirectes existent.

b. L'utilité de la surveillance de l'accès Internet avec l'obtention des informations concernant l'adresse IP ou l'adresse MAC

2105 La demande de renseignement relative à l'adresse IP s'accompagne souvent d'une surveillance des télécommunications occasionnant, notamment, le transfert des données envoyées ou reçues par le biais de l'accès surveillé. Quant à l'adresse MAC, elle ne fait pas l'objet d'une demande de renseignement, mais, lors d'une surveillance des télécommunications, le fournisseur d'accès Internet met à disposition et transmet simultanément ou périodiquement les données relatives aux paramètres de communication des équipements terminaux et les paramètres pour l'identification de l'abonné, notamment l'adresse MAC. Il va s'en dire que, couplée avec une surveillance des télécommunications et la transmission de données, un bon nombre d'informations précieuses – notamment, celles qui font l'objet de l'utilité de la surveillance sur Internet – à l'enquête et/ou à la procédure pénale peuvent être obtenues.

2106 Dans le cadre de cette partie de notre étude, nous nous limitons aux renseignements d'identification soit à l'aide de l'adresse IP, soit à l'aide de l'adresse MAC, les autres informations ayant déjà fait l'objet d'une analyse[1621].

2107 Par conséquent, grâce à l'adresse IP et/ou MAC, il semble possible d'identifier l'utilisateur d'une connexion Internet et/ou d'identifier l'équipement électronique utilisé.

[1621] Supra Partie II, Chapitre 3, I, A, n° 1101 ss.

c. L'utilité de la perquisition des documents électroniques et leur exploitation comme moyen de preuve

2108 Lors de l'analyse des dispositions légales relatives à la perquisition, notamment des supports informatiques, nous avons énoncé que de nombreux fichiers informatiques de diverses natures peuvent faire l'objet de cette mesure de contrainte. Nous ne revenons donc pas sur ce point et nous nous limitons à expliciter l'utilité de certains de ces fichiers.

2109 Les documents enregistrés sur un support informatique, tels que des fichiers Word, Excel, Powerpoint, les "logs" des conversations de messageries instantanées ou des fichiers audio ou vidéo peuvent contenir des informations sur la préparation d'un acte délictuel, sur le déroulement d'une infraction déjà commise ou peuvent être l'objet ou le résultat d'une infraction. Ainsi, si leur contenu permet de connaître des informations pertinentes sur une affaire pénale, il ne fait nul doute qu'ils sont utiles à la recherche de la vérité matérielle et servent de moyen probatoire pour élucider les faits. En outre, il n'est pas impossible qu'un ou des noms et prénoms apparaissent permettant de relier un ou des auteurs à une infraction déterminée.

2110 Les emails situés dans la boîte de réception, d'envoi, dans les brouillons ou dans la corbeille peuvent, corrélativement aux documents, être riches en informations. En outre, si l'adresse email de l'envoyeur et/ou du destinataire est connue, voire que l'adresse contient le nom, prénom et éventuellement le lieu de travail (prénom.nom@nom_de_domaine_de_l_entreprise.com), il est possible d'identifier le ou les individus.

2111 Les historiques Internet sont une troisième source d'informations utiles à l'enquête. Ils servent à l'autorité compétente pour découvrir quels sites ont été visités, quand et combien de fois au cours des derniers jours, semaines ou mois. Ainsi, il est possible d'accéder à un forum de discussion ou un service d'échange d'informations qui peuvent contenir des messages de la personne suspectée pertinents pour l'enquête ou encore d'afficher des pages Web présentant des méthodes pour commettre un acte illicite ou dont le contenu n'est pas légal, voire de découvrir un blog ou un site Internet personnel du suspect relatant ce qu'il a fait ou veut faire, etc.

2112 Enfin, les cookies sont des marques de passage de l'utilisateur d'un matériel informatique sur les sites Internet. Certains enregistrent simplement des informations sur la préférence de l'utilisateur et/ou des références de facturations, alors que d'autres stockent les mots de passe et login utiles à l'authentification. Ce dernier type de cookies est particulièrement intéressant pour l'autorité pénale. En effet, grâce à eux, ils peuvent accéder au contenu de

groupe de discussion fermé, à certains réseaux sociaux dont l'accès est interdit ou limité au public, tel que Facebook, et/ou de lire les messages privés sis sur ces pages web.

d. La conclusion sur l'efficacité et l'utilisation comme preuve des moyens informatiques

2113 Avec les possibilités qu'offrent les technologies informatiques, nous n'avons pas été exhaustifs sur tous les éléments de preuve pouvant être découverts à l'aide de la surveillance sur Internet, de la surveillance de l'accès Internet et de la perquisition des supports informatiques. Cependant, nous pouvons en déduire une conclusion globale sur l'emploi en procédure pénale des moyens informatiques.

2114 Pour autant que la procédure pour ordonner, autoriser et exécuter ces mesures de contrainte soit respectée, les documents, enregistrements ou données identificatrices sont admissibles comme éléments probatoires au procès pénal pour identifier les auteurs d'infractions et/ou pour déterminer les circonstances de certaines infractions.

2115 Les données issues des moyens informatiques étant des preuves dites matérielles, leur valeur probatoire dépend étroitement de leur authenticité et de leur véracité. Une preuve modifiée risque de ne pas relater la vérité, mais une vérité subjective et en réalité erronée. C'est pourquoi il faut déterminer l'influence des risques techniques et humains pouvant affaiblir la sécurité ou l'exactitude des données ainsi que l'influence des programmes, tels que les chevaux de Troie, afin de connaître la réelle force probante des moyens informatiques.

5. La discussion sur la preuve informatique

2116 A la différence des précédentes discussions sur les avantages et les problématiques des techniques comme moyen de preuve, la discussion sur la preuve informatique se cible sur les problématiques ou plus particulièrement sur les risques techniques et humains.

2117 Ce choix est motivé par divers éléments. Premièrement, les avantages de la preuve informatique sont similaires à ceux qui prévalent pour les autres preuves techniques[1622]. Deuxièmement, l'actualité récente sur les failles et risques informatiques alimentent les débats sur l'authenticité des données.

[1622] Supra Partie II, Chapitre 3, I, A, 4, a, n° 1254 ss; Supra Partie II, Chapitre 3, I, B, 4, a, ii, n° 1592 ss; Supra Partie II, Chapitre 3, II, E, 1, a, ii, n° 1786 ss.

2118 En pratique, les juristes combattent particulièrement fortement la preuve informatique plus que toutes autres. En effet, lorsqu'ils sont confrontés à une preuve informatique contraire à leurs allégués, ils tentent de décrédibiliser les moyens électroniques en attaquant les faiblesses de l'identification sur Internet et en pointant la vulnérabilité des technologies informatiques[1623].

a. Les problématiques liées à la surveillance sur Internet

i. L'incapacité de surveiller Internet de manière préventive

2119 Un moyen de surveillance peut être une mesure préventive ou répressive selon qu'une procédure pénale soit ou non pendante.

a) Les changements depuis l'entrée en vigueur du CPP

2120 Avec l'entrée en vigueur du Code de procédure pénale, l'aLFIS a été abrogée en faveur de l'édiction des art. 285a à 298d CPP relatifs à l'investigation secrète. Ces articles reprennent le contenu de l'aLFIS à ceci près qu'ils ne distinguent plus les deux phases d'investigation que l'aLFIS connaissait, à savoir la phase de procédure pénale (art. 14 ss aLFIS) et la phase précédant l'ouverture d'une procédure durant laquelle le commandement de la police pouvait ordonner une investigation secrète (art. 5 al. 1 aLFIS)[1624].

2121 Le législateur justifie l'abandon de cette distinction, par la contradiction du régime prévu dans l'aLFIS. En effet, l'art. 4 aLFIS prévoyait l'intervention d'agents infiltrés avant l'ouverture d'une procédure pour élucider si l'une des infractions énumérées avait été commise. Pour cela, des soupçons sur la réalisation de faits déterminés étaient nécessaires. Malgré que l'aLFIS ne réclamait par l'ouverture d'une procédure pénale, dans les circonstances prévues par l'art. 4 aLFIS, il était toujours possible d'en ouvrir une (art. 309 ss CPP).

2122 En outre, la surveillance purement préventive est illégale à la lumière du Code de procédure pénale car, ne nécessitant pas de soupçons, il s'agirait d'une recherche de preuves au hasard ou du *fishing expédition* contraire aux valeurs d'un Etat de droit.

[1623] CAPRIOLI Eric, L'archivage électronique: de la dématérialisation à la politique d'archivage, l'omniprésence du droit, disponible sur: http://www.caprioli-avocats.net/ [consulté le 08.05.2016].

[1624] JOSITSCH, Chatroom, p. 181 et 187; Message, CPP, p. 1238; SKARUPINSKI, GROSSENBACHER, n° 14.

b) La conséquence de la nouvelle réglementation sur les enquêtes réalisées sur un chatroom ou un forum de discussion

2123 Selon la jurisprudence[1625], la surveillance et l'établissement d'un contact sur Internet relèvent de l'investigation secrète ou des recherches secrètes. Avec l'abrogation de l'aLFIS, la situation lors d'enquête sur un *chatroom* n'est pas convaincante.

2124 En effet, au sens de l'art. 285a ss CPP, une investigation secrète ne peut être ordonnée qu'en présence de soupçons laissant présumer qu'une infraction listée à l'art. 286 al. 2 CPP ait été commise et qu'une procédure pénale soit ouverte (art. 1 al. 1 CPP). Ce constat vaut de même pour les recherches secrètes (art. 298b CPP). Par conséquent, contrairement à l'aLFIS, l'investigation secrète ou les recherches secrètes ne sont plus admissibles durant une simple phase d'enquête[1626] et une investigation préventive n'est pas non plus possible.

2125 Conformément à l'art. 123 al. 1 Cst, seule la législation en matière de procédure pénale relève de la compétence de la Confédération, ce qui signifie qu'en l'absence d'ouverture d'une procédure les mesures servant à prévenir les infractions ou à établir qu'elles peuvent être commises relèvent du droit de la police. La compétence législative revient alors aux cantons[1627].

2126 La situation législative cantonale n'est pas satisfaisante en ce qui concerne la poursuite des infractions et empêche bon nombre d'enquêtes.

2127 Les enquêtes préventives ont fait leurs preuves en tant qu'instruments efficaces pour recueillir des preuves et lutter efficacement, notamment contre la criminalité pornographique ou la délinquance pédophile[1628]. Sur Internet, les investigations réalisées sont majoritairement préventives, soit avant même l'existence d'un soupçon[1629].

2128 Malheureusement, actuellement, en l'absence de législation cantonale sur la police, une mesure de surveillance préventive sur Internet est illégale[1630]. Il n'est donc provisoirement

---

[1625] ATF 134 IV 266, 277 = JdT 2008 IV 35, 50-51.

[1626] SCHUBARTH, Jusletter, n° 5-6.

[1627] JOSITSCH, Chatroom, p. 188; Rapport du Conseil fédéral sur l'initiative n° 08.458, p. 5185; SCHUBARTH, Jusletter, n° 7; SKARUPINSKI, GROSSENBACHER, n° 24.

[1628] SCHUBARTH, Jusletter, n° 3-4.

[1629] JOSITSCH, Chatroom, p. 181; SKARUPINSKI, GROSSENBACHER, n° 14.

[1630] ATF 140 I 353, 362-364 = JdT 2015 I 39, 46-48

plus possible de lutter adéquatement contre certains types de criminalité, alors même qu'un moyen ayant démontré son efficacité existe.

ii. Les données interceptées par un Cheval de Troie introduit par l'autorité pénale

2129 Les programmes du type chevaux de Troie s'implantent dans la structure du système informatique d'un utilisateur. Ce type de programme permet à un tiers *in casu* à l'autorité pénale de contrôler l'appareil électronique et d'obtenir le transfert de certaines données utiles à l'enquête et à la procédure.

2130 Durant l'analyse de l'interception des conversations effectuées *via* le protocole TCP/IP, nous avons déjà fait état des risques pour l'authenticité des données recueillies inhérents à l'utilisation d'un logiciel espion[1631]. Le constat réalisé vaut *mutatis mutandis*.

2131 Dès lors, pour s'assurer d'une validité suffisante de la preuve, il faut impérativement que le logiciel introduit ne modifie que le support où sont inscrites les données et non pas les données elles-mêmes. Il ne doit en outre pas créer une faille de sécurité qui pourrait mener des tiers à s'introduire également dans le système de manière malveillante.

iii. Le vol d'identité et des accès

2132 Il existe tout un arsenal de méthodes d'attaques pour commettre des infractions *via* les technologies informatiques ou pour garder l'anonymat.

2133 L'une de ces techniques qui peut mettre à mal une identification sur Internet est la mystification ou *Spoofing*. Cette méthode consiste à prendre l'identité d'un tiers ou d'une autre machine électronique. Il peut s'agir de voler le nom de domaine URL d'un site Web (*Slamming* ou *URL Spoofing*), de récupérer le nom d'utilisateur et le mot de passe (*Login Spoofing*) ou de pirater l'adresse IP (*Spoofing IP*)[1632].

2134 Généralement, l'usurpateur emploie un cheval de Troie pour obtenir les informations désirées. Lorsque le nom d'utilisateur et le mot de passe sont entrés, l'information est enregistrée.

[1631] Supra Partie II, Chapitre 3, I, A, 4, c, i, d), n° 1347 ss.

[1632] BUQUET, p. 332. A ce sujet voir: MILLER Frederic P, VANDOME Agnes F, MCBREWSTER John, *IP Address Spoofing*, Sarrebruck 2011. Infra Partie II, Chapitre 3, III, A, 5, b, iii, n° 2158-2160.

2135 L'ingénierie sociale est une autre méthode ayant également pour conséquence l'usurpation du nom d'utilisateur et le mot de passe. Cette pratique exploite les failles humaines et sociales en manipulant les utilisateurs qui, naïvement, exécutent ce que l'usurpateur leur demande[1633].

2136 De manière générale, l'ingénierie sociale se déroule en premier par une phase d'approche qui met l'utilisateur en confiance. Il s'agit souvent, pour l'usurpateur, de se faire passer pour une personne hiérarchiquement supérieure, un client, un proche, etc. Ensuite, l'usurpateur met en alerte l'utilisateur souvent avec un faux prétexte de sécurité. Ainsi, la personne manipulée fournit elle-même les données confidentielles et personnelles, notamment les noms d'utilisateur et les mots de passe.

2137 Le hameçonnage ou *Phishing* est une troisième technique fréquemment employée pour obtenir les renseignements dans le but de perpétrer une usurpation d'identité[1634]. Cette technique est une sous-catégorie de l'ingénierie sociale. Il s'agit de se faire passer pour une autorité digne de confiance afin que la personne se rende sur un site internet et entre les données désirées.

2138 L'usurpation d'identité peut avoir des conséquences importantes sur l'élément probatoire plus spécifiquement sur l'identification d'un auteur. Prenons deux exemples pour expliciter cette affirmation.

2139 Un utilisateur d'Internet emploie quelque fois sa carte de crédit, notamment pour effectuer des achats et payer *via* la plateforme Paypal. Un jour, il découvre un email dans lequel une société se présentant comme la société Paypal lui demande pour des raisons de sécurité d'entrer son nom d'utilisateur, son mot de passe et de confirmer son numéro de carte de crédit, la date de validité et le numéro de sécurité. Incrédule, l'utilisateur s'exécute. Par la suite, cette carte de crédit est employée de manière malveillante pour payer un abonnement à un site pédopornographique. Une identification à l'aide de cette donnée est alors totalement erronée.

2140 Autre exemple, un utilisateur se voit usurper son login et son mot de passe par la méthode de mystification et pirater son adresse IP par la même technique. Ainsi, si l'usurpateur télécharge des fichiers illégaux à l'aide des données volées ou atteint à l'honneur d'un tiers en employant le profil de l'utilisateur qui ne se cache pas derrière un pseudonyme – par exemple sur Facebook –, là encore l'identification ne reflète alors pas la réalité.

[1633] BONDALLAZ, protection des personnes, p. 36-37; MONNIER, Hacking, p. 130; MONNIER, Piratage, p. 147.

[1634] BUQUET, p. 331 STUCKI, n° 1 et 11-13.

2141 L'utilisateur confronté au vol de ses données dans le premier exemple pourra relativement facilement démontrer qu'il ne s'agit pas de lui, notamment à l'aide de l'adresse IP utilisée par l'usurpateur. L'utilisateur du second exemple se trouve dans une position plus délicate, car même si aucun fichier n'apparaît sur un support informatique dont il est propriétaire cela n'exclut pas qu'il l'ait effacé. La situation est encore plus complexe si nous couplons les deux exemples. En effet, plusieurs éléments – carte de crédit, nom d'utilisateur, mot de passe et adresse IP – convergent alors vers une et unique identité.

2142 Partant de ce constant, l'identification sur un réseau social, un forum de discussion ou sur toute autre page Web n'est fiable que moyennant la prise en considération des risques d'usurpation et de leur exclusion dans le cas concret. Il est donc préférable que les éléments probatoires déterminés par les données informatiques soient confirmés par d'autres éléments probatoires.

b. Les problématiques liées à la surveillance de l'accès Internet

i. L'accès Internet depuis un réseau public, depuis un cybercafé, depuis le domicile d'un tiers ou par l'intermédiaire d'un routeur

a) L'accès depuis un réseau public, un cybercafé ou le réseau d'une entreprise

2143 L'une des principales difficultés dans l'identification d'un utilisateur d'accès Internet est l'appartenance même de l'adresse IP. En effet, l'adresse IP ne fournit pas une identification effective de l'utilisateur soupçonné et/ou de l'auteur de l'infraction, mais uniquement de la personne ayant contracté un abonnement auprès d'un fournisseur d'accès.

2144 Ainsi, si un criminel emploie un réseau d'accès gratuit et public, s'il se connecte depuis un cybercafé – sans être un client habituel et/ou connu et en payant cash – ou s'il utilise le réseau d'une entreprise, il n'est pas possible d'identifier l'utilisateur, mais uniquement l'abonné. En effet, un ordinateur est connecté sur Internet à travers un routeur. En amont du routeur, toute une série d'usagers peuvent être reliés à cet appareil. L'adresse IP interceptée est celle de l'accès, soit celle du routeur qui est connecté directement, et non pas celle des ordinateurs qui se cachent derrière celui-ci.

2145 Bien entendu, lorsque l'adresse IP d'une entreprise est détectée, il est toujours possible de perquisitionner tous les postes de travail même si la tâche peut être longue et fastidieuse selon le nombre d'employés. Néanmoins, il n'est pas exclu qu'aucune trace de l'infraction ne soit visible parce qu'effacée ou enregistrée sur un support mobile. A noter que les entreprises

n'ont pas le droit de surveiller un employé et par conséquent ne peuvent pas déterminer quel est l'ordinateur qui a envoyé ou reçu un certain flux de données. Il faudra alors, éventuellement, s'intéresser au réseau interne de l'entreprise afin d'obtenir plus d'informations.

2146 Ce constat est plus problématique que réellement dangereux en procédure pénale. En effet, sans identification, il n'y a aucun risque de voir un innocent identifié, mais sans identification, il ne peut y avoir de suspect.

b) En cas d'utilisation d'un accès Internet familial ou d'un tiers

2147 Dans ce cas de figure, la problématique est la même que celle exposée ci-dessus à ceci près que le nombre d'utilisateurs effectifs est plus restreint.

2148 Concernant l'utilisation d'un accès Internet familiale, l'adresse IP sortante est celle du routeur derrière lequel peut être connecté plusieurs ordinateurs ou appareils électroniques. L'identification de l'usager est donc, en tant que telle, inutile, puisqu'en tout état de cause, elle concernera le contractant du service et non pas le suspect ou l'auteur.

2149 Ainsi, l'adresse IP n'est pas une preuve suffisante, il faudra encore perquisitionner les supports informatiques afin de contrôler qui est l'auteur d'un acte délictuel. Cependant, il n'est pas exclu qu'aucune réponse ne puisse être apporté. Outre l'utilisation d'un support mobile pour enregistrer des données qui ne serait pas trouvé, il n'est pas rare que, malgré la possibilité d'avoir un login sécurisé, les membres d'une même famille emploient la même session système ou qu'un ou plusieurs ordinateurs ne soient pas sécurisés par un mot de passe. Il n'est alors pas possible d'identifier qui est l'auteur de l'infraction.

2150 Notons par ailleurs que tout possesseur d'un ordinateur ne peut pas se voir inculper pour possession d'image pornographique au sens de l'art. 197 ch. 3*bis* CP du seul fait que le support informatique lui appartient. La Tribunal fédéral a relevé que cette infraction nécessitait – comme toutes infractions consommées – l'accomplissement de l'élément objectif et subjectif. Un utilisateur d'ordinateur ou d'Internet qui ignore que des données tombant sous le coup de l'art. 197 ch. 3*bis* CP sont présents dans son ordinateur – parce que le dossier est sécurisé, que les données sont sises dans la mémoire cache ou simplement que les données sont dans un dossier visible mais dont la personne n'a pas connaissance – n'agit pas intentionnellement faute de conscience et de volonté de les posséder[1635].

[1635] ATF 137 IV 208, 214-215 = JdT 2012 IV 114, 120.

2151 Autre est la problématique d'un utilisateur qui emploie la connexion d'un proche ou d'un ami pour commettre un méfait. A nouveau, la personne qui sera identifiée à l'aide de l'adresse IP est le proche ou le tiers. Imaginons que ces derniers transmettent fréquemment leur mot de passe d'accès WiFi, il devient quasiment impossible de déterminer qui a employé le réseau et ainsi d'identifier l'auteur d'une infraction. En tout état de cause, un travail d'enquête poussé devra être effectué pour obtenir plus d'indices et d'éléments pertinents.

ii. L'accès Internet non sécurisé

2152 Le Wired Equivalent Privacy abrégé WEP est un protocole pour sécuriser les réseaux sans fil de type WiFi afin d'éviter les écoutes clandestines ou le piratage de la ligne Internet[1636]. La clé WEP est une clé de chiffrement qui peut se comparer à un mot de passe composée de chiffres et de lettres propres à chaque routeur. Cette clé sécurise l'accès Internet en limitant la connexion au routeur aux seuls utilisateurs connaissant la clé.

2153 Le WiFi Protected Access abrégé WPA est également un mécanisme de sécurité réseau sans fil de type WiFi qui fonctionne de manière similaire[1637].

2154 Sans clé WEP ou WPA, le réseau WiFi est ouvert à tous. Ainsi, une personne disposant d'un ordinateur portable ou d'un autre appareil électronique disposant du WiFi peut détecter le réseau non sécurisé et se connecter sur Internet à l'aide de l'accès d'autrui.

2155 En cas d'infraction, la personne identifiée sera le propriétaire de la ligne Internet non sécurisée et non pas le réel auteur de l'acte. En cas d'accès répéter sur le réseau non-sécurisé, il faudra investiguer pour découvrir si la connexion réseau est employée par un voisin ou par une autre personne se trouvant fréquemment proche de l'accès WiFi. Dans le cas contraire, il n'est pas impossible que le crime reste impuni.

2156 Relevons encore que malgré la protection du routeur par une clé WEP ou WPA, il n'est pas exclu qu'un tiers non autorisé se connecte sur le réseau WiFi protégé. En quelques minutes, moyennant quelques recherches sur Internet, la procédure pour cracker une clé WEP et WPA est accessible à tout un chacun[1638]. Ainsi, n'importe qui ayant un minimum de connaissances en informatique peut employer le réseau WiFi d'un tiers.

[1636] DOCTER, DUNALEY, SKANDIER, p. 345; GAST, p. 121; MARTIN K., p. 427.

[1637] DOCTER, DUNALEY, SKANDIER, p. 345; GAST, p. 160; MARTIN K., p. 431.

[1638] A ce sujet, voir: Le procès-verbal de constat rédigé par Me Eric Albou, huissier de justice à Paris, disponible sur: http://static.pcinpact.com/pdf/annexe1-constat-ufc-que-choisir-wifi.pdf [consulté le 08.05.2016].

2157 En outre, les failles des systèmes d'exploitation peuvent être utilisées par un auteur d'infraction pour piloter à distance un autre ordinateur et faire croire que c'est ce dernier qui interagît sur le réseau. Couplé avec un système TOR – réseau mondial décentralisé de routeurs qui permettent de transmettre anonymement des flux TCP –, il n'est plus possible de tracer le réel coupable ou même simplement de savoir qu'il existe[1639].

iii. La duplication des adresses IP et/ou de l'adresse MAC

2158 L'adresse IP ne permet pas d'identifier l'utilisateur effectif du réseau au surplus, elle ne permet pas non plus de s'assurer que le routeur censé être connecté par cet IP est bien le seul et l'unique.

2159 L'usurpation d'adresse IP ou l'IP *Spoofing* est une méthode répandue sur Internet. Cette technique consiste à remplace l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'un autre routeur. Corrélativement à la sécurité relative de l'accès WiFi qui nécessite quelques minutes pour être "cracké", en peu de temps un utilisateur peut se connecter anonymement sur Internet ou plus exactement sous le couvert d'une autre identité.

2160 Notons que l'utilisation d'un duplicata ne rend pas impossible l'utilisation simultanée par l'utilisateur originel et le hacker de la connexion Internet. Dans un tel cas de figure, un message alerte le fournisseur d'accès et l'utilisateur que l'adresse IP est employée deux fois, ce qui peut permettre de prendre en considération ce facteur en cas de demandes de surveillance et d'identification de l'usager. En revanche, si le duplicata n'est pas utilisé en même temps, rien n'indique qu'il existe.

2161 Le contrôle d'accès au réseau informatique basé sur l'adresse MAC n'est pas plus probant. La technique du MAC *Spoofing* offre la possibilité de paramétrer l'adresse MAC et donc de la modifier. Couplé avec quelques commandes sous UNIX, il est possible de détecter les adresses IP et les adresses MAC environnantes. Ainsi, l'utilisateur usurpant l'adresse IP et l'adresse MAC devient totalement invisible et passe pour un tiers.

2162 En outre, il existe divers autres procédés permettant de modifier l'adresse MAC sur une machine. Par exemple, sous Windows XP, si le pilote le permet, sous l'onglet "avancé" des propriétés de la carte réseau, il est possible d'affecter une autre adresse MAC en quelques clics de souris.

[1639] DAS, KANT, ZHANG, p. 32; LATHOUD, p. 185 et 189.

2163 Par conséquent, l'adresse IP et/ou l'adresse MAC ne démontrent rien, hormis peut-être l'existence systématique d'un doute.

c. Les données issues de la perquisition sur un support informatique

i. La vulnérabilité des systèmes d'exploitation

2164 Les systèmes d'exploitation, malgré l'utilisation de sécurités, de logiciels anti-virus ou de programmes anti-malware, sont vulnérables et sujets à des attaques extérieures pouvant décrédibiliser la validité des données informatiques perquisitionnées, dès lors que leur intégrité n'est plus garantie[1640].

2165 Les attaques par logiciels malveillants – virus, vers, chevaux de Troie, etc. – ou logiciels espions vont infecter le système informatique à l'insu de l'utilisateur. Diverses variantes existent et ne cessent d'évoluer pour déjouer la sécurité des anti-virus. Nous énonçons les attaques les plus fréquentes et les conséquences qu'elles peuvent avoir sans pour autant être exhaustif sur les méthodes possibles.

2166 La modification de données est la méthode la plus simple, la plus sûre et la plus courante en matière de criminalité informatique. Elle peut être effectuée manuellement par toutes personnes participant ou ayant accès au processus de création, d'enregistrement, de codage, d'analyse, de conservation ou de transformation des données informatisées[1641]. Il est ainsi possible d'obtenir des documents falsifiés.

2167 Les virus et les vers sont des programmes malveillants conçus pour pénétrer dans des systèmes et se dupliquer. Ce type de logiciels malveillants n'a que peu d'impact sur la preuve informatique dès lors qu'ils ne font que détruire les données.

2168 Les kits racines ou *Rootkits* offrent les droits d'administrateur sur une machine afin d'installer une porte dérobée (voir l'explication sous la description des chevaux de Troie), de truquer les informations et d'effacer certaines traces – historiques, chronologies, journaux, etc. – à distance.

[1640] CAPRIOLI Eric, L'archivage électronique: de la dématérialisation à la politique d'archivage, l'omniprésence du droit, disponible sur: http://www.caprioli-avocats.net/ [consulté le 08.05.2016]; FURNER, p. 210; LATHOUD, p. 189; TRECCANI, p. 226.

[1641] BUQUET, p. 327.

2169 Les chevaux de Troie ont déjà fait l'objet de notre étude[1642], nous revenons donc brièvement sur le sujet. Le programme parasite réalise des tâches non-autorisées sur l'ordinateur infecté qui continue pour autant à fonctionner normalement. Il existe plusieurs sous-catégorie de chevaux de Troie, notamment les "portes dérobées" qui sont les chevaux de Troie les plus dangereux, les plus répandus et ceux qui créent le plus de risques pour l'authenticité des fichiers informatiques. Il s'agit d'un utilitaire d'administration à distance qui permet de prendre le contrôle de l'ordinateur et ainsi d'intégrer des fichiers, des données, de les modifier ou d'intercepter des informations confidentielles comme les mots de passe[1643].

2170 Le super-zapping est un programme utilitaire permettant de modifier des fichiers.

2171 Ces quelques exemples de logiciels espions nous mènent à un seul constat: les systèmes d'exploitation ne sont pas protégés contre tous les risques et les données informatiques ne sont ni fiables, ni inaltérables, ni forcément authentiques. En cas d'utilisation des informations enregistrées sur supports informatiques, des mesures tangibles de vérification pour s'assurer de l'originalité des données, notamment en combinant les données informatiques avec d'autres types de preuve, doivent être prises sans quoi le doute ne peut pas être ôté[1644].

ii. L'incapacité générale d'authentifier les données informatiques

2172 Nous l'avons énoncé ci-dessus toute une série de moyens peuvent mettre à mal l'authenticité des fichiers informatiques[1645]. En effet, actuellement, il est difficile, en l'absence de signature électronique, de prouver qu'il existe aucune modification ou manipulation d'une preuve informatique[1646].

2173 La signature électronique est un procédé qui permet de déterminer l'origine du document électronique et de vérifier qu'il n'a pas été modifié[1647]. Il est ainsi possible de prouver l'authenticité et l'intégrité du document signé électroniquement.

2174 L'admissibilité de l'écrit électronique est par ailleurs étendue à l'acte authentique sous forme électronique. Il dispose de la même force probante que l'acte authentique sur support papier

[1642] Supra Partie II, Chapitre 3, I, A, 4, c, i, d), n° 1347 ss; Supra Partie II, Chapitre 3, III, A, 5, a, ii, n° 2128 ss.

[1643] BUQUET, p. 327 et 328; TRECCANI, p. 226.

[1644] FURNER, p. 210-211.

[1645] Supra Partie II, Chapitre 3, III, A, 5, c, i, n° 2164 ss.

[1646] LATHOUD, p. 190.

[1647] FISCHER, KUHN, p. 6-7; JACCARD, p. 120 ss; Message, SCSél, p. 5428; MÜLLER Jérémie, p. 251.

sous réserver, notamment, que le fichier soit établit en respectant une certaine procédure (art. 10, 11 et 13 OAAE[1648]) et que la signature électronique soit apposée par l'officier public (art. 3 al. 1 let. d OAAE).

2175 Cependant, il nous faut relever qu'en 2008, soit avant l'introduction de l'ordonnance sur les actes authentiques électroniques, des chercheurs en sécurité indépendants, notamment de l'EPFL, ont trouvé des failles dans l'infrastructure du certificat électronique. Une équipe chinoise a réussi à créer une attaque dite de collision et a pu créer deux messages différents avec une même signature électronique[1649]. Certes, le MD5 – algorithme utilisé pour certaines signatures électroniques – n'est quasiment plus exploité; néanmoins, il n'est pas exclu que le SHA-3 fasse également l'objet de faille que les hackers découvriront rapidement[1650]. Il est, également, utile de relever que le SwissID – signature électronique utilisée en Suisse qui répond aux normes en vigueur (Loi fédérale du 19 décembre 2000 sur les services de certification dans le domaine de la signature électronique (SCSE), RS 943.03) – a fait l'objet d'un piratage en 2010.

2176 Ce constat remet en cause la valeur scientifique ou technique des moyens informatiques qui peuvent facilement être décrédibilisés. Dès lors qu'il n'est pas possible de prouver qu'un fichier est un original qui n'a subi aucune modification, la défense pourra facilement émettre un doute permettant l'acquittement de l'accusé.

2177 Ainsi, comme toute preuve analysée jusqu'à présent, la nécessite d'un faisceau d'indices et de moyens probatoires est essentiel.

6. Une perspective d'avenir – L'espion clavier

2178 Depuis quelques années, un nouveau produit est apparu: l'espion clavier, enregistreur de frappe ou *keylogger*, permettant d'intercepter des informations directement depuis l'ordinateur d'une personne surveillée.

[1648] Ordonnance du 23 septembre 2011 sur l'acte authentique électronique (OAAE), RS 943.033.

[1649] Informations disponibles sur le site de l'EPFL: http://actualites.epfl.ch [consulté le 08.05.2016].

[1650] Informations disponibles sur le site de l'EPFL: http://actualites.epfl.ch [consulté le 08.05.2016].

a. Qu'est-ce que l'espion clavier?

2179 Il existe deux types d'espion clavier: logique ou matériel[1651]. Tous deux se définissent comme un processus furtif qui est chargé d'enregistrer les touches frappées sur le clavier.

2180 L'espionnage logiciel ou espion clavier logique est un programme inoffensif et invisible de l'utilisateur qui enregistre les frappes dans un fichier du disque dur. Si le logiciel est couplé avec un cheval de Troie, il les transmet directement à un tiers *via* le réseau. Dans le cas contraire, le fichier peut être récupéré directement sur l'ordinateur. Ce logiciel s'installe soit directement, soit par le biais d'un logiciel type cheval de Troie. L'utilisation d'un pare-feu peut permettre de contrecarrer les risques d'un espion clavier logique.

2181 L'espionnage par matériel ou espion clavier matériel ne peut pas être déjoué par un pare-feu, mais demande d'avoir accès au matériel informatique. Pour pouvoir intercepter les touches frappées par un utilisateur, il suffit d'ajouter un dispositif – câble ou dongle (clé électronique) – entre le port de branchement du clavier et le clavier lui-même. Quant au clavier sans fil, il suffit de capter les ondes émises entre le clavier et le récepteur, et de les déchiffrer. En outre, le dispositif matériel peut ou non être pourvu d'un émetteur afin de transmettre en direct l'information à l'observateur.

b. L'utilité de l'espion clavier en procédure pénale

2182 L'utilité de la surveillance policière et judiciaire des messages électroniques n'est plus à prouver. L'espion clavier offre un nouveau moyen de surveillance.

2183 Niklaus Schmid considère que l'utilisation des ondes électromagnétiques et l'usage d'un espion clavier relève de l'art. 280 let. b CPP[1652]. Il considère que l'espion clavier matériel est un dispositif technique de surveillance qui permet d'enregistrer des actions.

2184 Néanmoins, l'interprétation de Niklaus Schmid semble aller trop loin sur un point. Comme le relève Thomas Hansjakob[1653], en accord avec Stefan Trechsel et Viktor Lieber[1654], l'enregistrement d'un autre dispositif technique doit être en relation avec un élément qui est observé. En l'espèce, l'espion clavier ne permet pas l'observation. En outre, l'espion clavier

[1651] BONDALLAZ, protection des personnes, p. 39; MOREILLON, BLANK, p. 81-82; TRECCANI, p. 234-236.

[1652] SCHMID, Praxiskommentar, art. 280 N 9.

[1653] StPO-HANSJAKOB, art. 280 N 15.

[1654] TRECHSEL, PIETH-TRECHSEL, LIEBER, art. 179*bis* N 7.

logique est un programme et non un dispositif qui ne serait donc pas inclus dans le champ d'application de l'art. 280 CPP[1655].

2185 Alors qu'aucune solution ne semble envisagée actuellement pour l'utilisation de l'espion clavier logique, la modification de la LSCPT et l'introduction de l'art. 269*ter* CPP permettront l'utilisation d'un logiciel qui capte et lit des données informatiques. Par conséquent, outre la possibilité de pouvoir utiliser les chevaux de Troie, l'art. 269*ter* CPP constitue la base légale justifiant l'ingérence aux droits fondamentaux créée par l'utilisation de l'espion clavier.

c. L'évolution du espion clavier avec l'espionnage à distance à l'aide des ondes électromagnétiques

2186 L'espion clavier est devenu une méthode de piratage couramment utilisée grâce aux logiciels de type *keyloggers*. En 2008, deux étudiants de l'EPFL ont trouvé une méthode pour faire parler les claviers sans utiliser de logiciels espions ni de dispositifs techniques[1656]. Il suffit d'intercepter les ondes électromagnétiques.

2187 Onze claviers filaires connectés par PS/2 – prise classique –, par USB ou raccordés à un ordinateur portable ont été testés. Les claviers étant tous conçus avec des composants électroniques, ils émettent des ondes électromagnétiques de faible portée. Ainsi, à une distance de 20 mètres, il est possible d'intercepter les ondes et de retranscrire les informations tapées.

2188 Même si la portée des ondes est faibles, ce processus offre la possibilité d'employer une faille qui ne peut être déjouée ni par un antivirus, ni par aucun pare-feu. Ainsi, si l'autorité pénale emploie ce moyen – à condition que cette technique soit prévue par la loi –, la personne surveillée n'aura pour seul moyen que de placer son clavier dans une cage métallique – cage de Faraday – pour ne pas voir ses frappes claviers interceptées.

2189 Précisons au surplus que cette méthode n'est encore ni prouvée par une autre étude, ni testée plus concrètement et à large échelle. Dès lors, les risques d'interférence, notamment, ne sont pas démontrés. Par conséquent, la fiabilité des données de frappes doit encore être établie pour déterminer si cette méthode peut faire l'objet d'un moyen de preuve suffisamment probant.

[1655] Supra Partie II, Chapitre 3, I, A, 4, c, i, b), n° 1309 ss.

[1656] Le Temps, *Comment espionner à distance un clavier*, article du 28 octobre 2008.

B. Les bases de données

> *"[Le développement de l'informatique] a suscité, en même temps que l'espérance d'une société mieux informée, plus prospère et plus libre, des appréhensions très sérieuses. […] l'informatique pouvant mettre à la disposition des personnes publiques et des entreprises privées, un assez grand nombre d'informations sur les particuliers […]"*[1657].

2190 Cette citation reprise de l'écrit de Jean Frayssinet et Pierre Kayser fait référence aux bases de données créées par les autorités compétentes ou par des entreprises privées.

2191 Le domaine de l'informatique offre de nouvelles perspectives rendant quasiment dépendantes les utilisateurs qui constatent une facilitation dans l'exercice de leurs tâches professionnelles et privées. La création de bases de données automatisées ne fait pas exception. Les entreprises, les personnes privées et l'administration recourent de plus en plus à cette méthode pour classer, rechercher, mettre à jour et transmettre les données, renseignements ou informations recueillies.

2192 La présente partie vise à placer l'utilisation des bases de données dans la perspective de la recherche criminelle relative à l'identité du ou des auteurs, à la comparaison d'indices, voire à leur corrélation. Après une présentation générale des bases de données et leur usage en Suisse par les autorités pénales ou les acteurs de la justice (1.-2.), nous axerons notre analyse sur les conflits pouvant exister entre les droits de la personnalité et l'exploitation de bases de données (3.) ainsi que sur les risques inhérents à la technicité de ce domaine informatique (4.). Puis, nous conclurons par le potentiel futur des bases de données (5.)

1. L'avènement des systèmes d'information

a. Les remarques générales

2193 Depuis de nombreuses années, la puissance des systèmes informatiques a considérablement progressé, les composants se sont miniaturisés et le coût du matériel informatique a chuté pour devenir accessibles à toutes les entreprises et aux particuliers. Les premiers disques durs en 1956 ont permis d'utiliser les ordinateurs pour collecter et stocker de grandes quantités d'informations. Avec le développement de la technicité des équipements utiles à la

[1657] FRAYSSINET Jean, KAYSER Pierre, La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret du 17 juillet 1978, in *Revue de droit public* 1978, p. 629.

transmission et au traitement des informations, l'intégration, la gestion et la recherche automatisée des données sont devenues qualitativement et quantitativement plus performantes.

i. Quelques notions techniques

2194 Au fil des années, le nombre d'informations automatisées a pris rapidement une telle ampleur qu'une hiérarchisation s'est imposée. Il s'ensuivit la création de divers types de systèmes de gestion de base de données (SGBD): hiérarchiques, réseaux, relationnels, orientés objet, XML natif, etc. Les SGBD permettent de stocker et d'organiser de manière structurée une grande quantité d'informations en garantissant la qualité, la pérennité et la sécurité des données.

2195 Au moyen de requêtes – ou "langages d'interrogation" –, il devient possible de naviguer et d'extraire facilement des informations consolidées. En d'autres termes, les SGBD sont des logiciels systèmes structurant et organisant le fonctionnement des bases de données.

2196 Quant aux bases de données elles-mêmes, elles sont constituées d'un élément statique – définissant leur structure – manière de stocker les données, comparable aux rangées d'armoires, aux rayons contenus dans une bibliothèque classique – et d'éléments dynamiques – la collection des données ainsi que des possibilités pour l'utilisateur d'accéder à la demande aux informations enregistrées[1658].

2197 S'ajoute encore, la possibilité actuelle de pouvoir numériser tout type de données – textes, images, sons, graphiques, etc. – grâce à l'informatique[1659]. Ainsi, un traitement à l'aide de la reconnaissance graphique ou de caractère est possible, ce qui permet d'effectuer des recherches en lien avec divers supports, modèles ou types de documents.

ii. La transmission des informations à distance

2198 La connexion transfrontalière a généré, en outre, un flux de données importants sans qu'aucune barrière technique ne puisse entraver la transmission[1660]. La voie télématique offre

[1658] DUCOR, p. 157; Glossaire des termes informatiques édité par IBM: http://www-01.ibm.com/ [consulté le 08.05.2016].

[1659] BONDALLAZ, protection des personnes, p. 15; DELOBEL, p. 83.

[1660] DUCOR, p. 155; DSG-EPINEY, p. 559; MEIER P., p. 436; WALTER, Données personnelles, p. 99.

ainsi un moyen de transport des messages ou des données entre deux ou plusieurs utilisateurs. Elle se compose d'un moyen de transmission, d'un équipement de transmission et de terminaux permettant le transfert et la réception des données de manière facilitée. Les réseaux internes, les réseaux sécurisés et le réseau Internet constituent donc la troisième cause expliquant le recours toujours plus fréquent à l'informatique.

2199 Dans notre domaine d'intérêt qu'est la procédure pénale, la communication locale ou nationale par réseau informatique a largement simplifié l'échange d'informations et de renseignements entre les autorités cantonales et l'administration fédérale, entre les autorités de divers cantons ou entre les services d'un même canton.

iii. Les généralités sur les données enregistrées, traitées et analysées

2200 Les systèmes d'informations nommés communément base de données sont considérés comme les moyens les plus aptes à conserver, traiter, rechercher et lier une quantité presque illimitée de données dans un temps réduit[1661]. L'unique limite à cette technique de traitements automatisés dépend du nombre de fiches, de données, de renseignements ou de toutes autres informations qui sont intégrés dans le système informatisé par le maître du fichier.

2201 Aux fins de l'exploitation d'un système d'informations, les données recueillies doivent être préparées ou prétraitées – notamment quand le format ou modèle des données n'est pas uniforme – pour être intégrées à la base de données et pouvoir être analysées[1662]. L'efficience d'un système d'informations dépend étroitement des données qui y sont intégrées. Sans donnée et en toute logique, un traitement est impossible et une recherche d'information ne fournira aucun résultat.

2202 La qualité, la validité et l'actualité des données enregistrées est un autre point d'orgue à l'utilité et à l'exploitabilité des bases de données. Une information inexacte ou inactuelle ne peut pas servir à l'autorité ou tout autre utilisateur.

2203 Si nous prenons l'exemple de la base de données de l'office cantonal des automobiles et de la navigation à Genève et que nous imaginons un changement du possesseur d'un numéro de plaque, l'identité du possesseur dudit numéro de plaque et son adresse doivent notamment être modifiées si tel n'est pas le cas les contraventions ou amendes sanctionnant une

[1661] DUCOR, p. 155; VITALIS, p. 55.

[1662] CAPT, p. 83; ELOY, p. 8.

violation des règles de la circulation routière sont envoyées au mauvais destinataire créant une situation inconfortable. Il est donc essentiel que les données intégrées soient correctes et mises à jour régulièrement pour que l'autorité puisse bénéficier adéquatement du système informatisé.

b. L'introduction des bases de données dans l'administration et dans le cadre des tâches des autorités en procédure pénale

2204 Les fichiers gérés manuellement ont perdu peu à peu de leur efficacité avec l'accroissement constant de la quantité de fiches et données recueillies et conservées. Les recherches effectuées manuellement ne pouvaient plus donner de résultat exhaustif ou moyennant des heures considérables de travail. L'introduction de l'informatique dans le cadre de l'administration et de la procédure pénale – comme partout ailleurs – s'est donc tout d'abord réalisée en automatisant les fichiers manuels existants afin de surmonter les difficultés rencontrées lors du traitement manuel.

2205 Dans une seconde phase, des systèmes d'informations se sont développés dans le dessein de regrouper, classifier, traiter et transmettre des données[1663]. Ainsi, il est possible d'automatiser les opérations de traitement, de recherche et de transmission, de lier les autorités pénales entre elles ou avec des services tiers, de rationnaliser l'échange d'informations et de coordonner les actions des diverses autorités. Par conséquent, en tant que système structuré et fonctionnant de manière autonome, les bases de données permettent l'utilisation rationnelle des informations recueillies et enregistrées.

2206 En tant que tels, les outils de renseignement informatisés et les bases de données des autorités fédérales ou cantonales ne sont pas des moyens de preuves. Néanmoins, en ce qu'ils sont utiles à la recherche ou au traitement d'un moyen probatoire, ces outils servent indirectement à l'administration de la preuve. A des fins judiciaires, l'utilisation des bases de données a permis notamment à ce que tous les indices scientifiques et techniques développés au cours de notre étude puissent être conservés et traités sous la forme de fichiers informatisés.

[1663] LAUDON, LAUDON, FIMBEL, COSTA, p. 20; MEIER A., p. 12.

2. Quelques bases de données fédérales

2207 Proposé en 1970 par le chercheur Edgar F. Codd d'IBM[1664], le modèle de base de données relationnelle, composée de diverses tables contenant des données et étant liées en entre-elles, s'est propagé rapidement. Le système JANUS, le système RIPOL, le système IPAS, la base de données AFIS, la base des données ADN CODIS, tous ces fichiers des autorités suisses utilisent un système de gestion relationnelle.

2208 Néanmoins, en vertu de la nature des données collectées, du nombre d'utilisateurs potentiels et du type d'utilisation désirée, une même information peut être présentée et/ou classée de diverses manières en fonction de l'usage qui en est fait et de sa mise en œuvre, notamment quant aux critères principaux ou secondaires de traitement et de recherche. Les bases de données sont donc *de facto* toutes différentes[1665].

2209 En Suisse, il existe un certain nombre de bases de données: privées ou publiques, communales, cantonales, intercantonales ou fédérales, etc. Physiquement et juridiquement, toutes ces bases de données ont leurs propres particularités. Il est difficile, voire impossible, d'être exhaustif quant au contenu matériel de ces systèmes informatisés ou au champ d'application juridique. Nous présenterons brièvement les principales bases de données intéressantes dans le cadre de notre étude et de la procédure pénale.

a. Le système informatisé de la Police judiciaire fédérale – JANUS

2210 Le système informatisé de la Police judiciaire fédérale nommé JANUS est un système d'informations commun aux divers secteurs qui relèvent de la compétence de la Division des offices centraux de police criminelle de l'Office fédéral de la police. La base de données JANUS est alimentée par les polices suisses qui se partagent donc les informations entre elles.

2211 L'ordonnance JANUS[1666] et les articles 10, 11, 12, 13 et 18 LSIP[1667] fondent les bases juridiques de la création de ce système d'informations composé de cinq sous-systèmes: le système d'appui aux enquêtes de police judiciaire de la Confédération, le système de

[1664] CODD Edgar F., A relational model of data for large shared data banks, in *Communications of the ACM* vol. 13 (1970) n° 6, p. 377-387.

[1665] DELOBEL, p. 83; DSG-BELSER, p. 40.

[1666] Ordonnance fédérale du 15 octobre 2008 sur le système informatisé de la Police judiciaire fédérale (O-JANUS), RS 360.2

[1667] Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP), RS 361.

traitement des données relatives aux infractions fédérales, le système d'appui aux enquêtes menées par les cantons dans leur domaine de compétence en matière de poursuite pénale, le système de gestion des affaires et des dossiers de l'Office fédéral de la police et le système de traitement des données relatives à la coopération policière internationale et intercantonale (art. 1 al. 2 O-JANUS *cum* 10, 11, 12, 13 et 18 LSIP).

2212 Les informations répertoriées ont pour but de permettre l'exécution des enquêtes relevant des domaines de compétence de la Confédération, de faciliter l'exécution des enquêtes préliminaires et des enquêtes de police judiciaire par les autorités cantonales de poursuite pénale et les services de police criminelle des cantons, et de faciliter la gestion des documents et des dossiers utilisés par la Fedpol.

2213 Pour atteindre ces buts, le système JANUS répertorie un certains nombres d'informations classées dans des sous-catégories: "Personnes et antécédents" où sont enregistrées des informations sur des personnes, des organisations et des personnes morales et leurs antécédents provenant d'enquêtes préliminaires, d'enquêtes de police judiciaire ou de sources accessibles au public; «Journaux» où sont enregistrées, affaire par affaire, des données provenant d'enquêtes préliminaires, d'enquêtes de police judiciaire ou de sources accessibles au public (notamment surveillances des télécommunications, mains courantes d'observation, mains courantes d'enquête); «Rapports de police» où sont établis et gérés les rapports et dénonciations nécessaires à l'accomplissement des tâches de la Police judiciaire fédérale; «Gestion des affaires et des dossiers» où sont enregistrées les données nécessaires au suivi des affaires; «Renseignements généraux» où sont enregistrées des données utiles à l'accomplissement des tâches telles que répertoires téléphoniques, extraits de presse, descriptifs des compétences de diverses administrations ou informations provenant de sources accessibles au public; «Rapport de situation» où sont enregistrés des rapports décrivant la situation nationale et internationale; «Analyses» où sont enregistrés les résultats des mandats d'analyse; «Fausse monnaie» où sont enregistrés les différents types de fausse monnaie et les techniques de faux monnayage; les données enregistrées en format texte, photo, vidéo ou audio réunies par la Police judiciaire fédérale dans le cadre d'enquêtes de police judiciaire portant sur des procédures pendantes; les données enregistrées en format texte, photo, vidéo ou audio réunies par la Police judiciaire fédérale dans le cadre d'enquêtes préliminaires (art. 5 O-JANUS).

2214 Grâce au nombre considérable de données variées intégrées dans cette base de données, les autorités peuvent détecter de manière précoce les infractions les plus graves ainsi que de

faciliter considérablement le travail de police[1668]. En effet, l'enquête criminelle cherche à reconstruire les événements en fonction de trois critères: les personnes et les objets concernés, les lieux et le moment. A l'aide de la base de données JANUS, il est possible de répertorier les faits constatés et de les mettre automatiquement en perspective.

b. Le système de recherches informatisées de police – RIPOL

2215 L'ordonnance RIPOL[1669] réglemente l'utilisation du système de recherche informatisé de la police.

2216 Le système de recherches informatisées de police appelé RIPOL est composé de trois bases de données exploitées conjointement par les autorités compétentes de la Confédération et des cantons. Une base de données concerne la recherche de personnes (art. 8 let. a *in limine* O-RIPOL), une deuxième concerne la recherche de véhicules (art. 8 let. a *in fine* O-RIPOL) et la troisième concerne les infractions non élucidées et la recherche d'objets (art. 8 let. b O-RIPOL).

2217 Les données inscrites dans RIPOL permettent le signalement et l'identification des personnes, des véhicules et des infractions non élucidées ou des objets recherchés (art. 8 à 11 O-RIPOL et art. 15 LSIP).

2218 Grâce aux informations enregistrées, le système RIPOL offre une assistance essentielle aux autorités fédérales et cantonales, notamment, pour arrêter des personnes ou rechercher le lieu de séjour dans le cadre d'une enquête pénale (art. 15 al. 1 let. a LSIP), ou pour effectuer une surveillance discrète ou un contrôle ciblé de personnes et de véhicules en vue de poursuivre une infraction pénale ou de prévenir des risques pour la sécurité publique (art. 15 al. 1 let. j LSIP)[1670].

[1668] CARTIER, RICPTS, p. 71; Message, LSIP, p. 4832 et 4838.

[1669] Ordonnance fédérale du 15 octobre 2008 sur le système de recherches informatisées de police (O-RIPOL), RS 361.0.

[1670] Message, complémentaire LPD, p. 1177-1178.

c. Le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police – IPAS

2219 Le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police abrégé IPAS repose sur les dispositions de l'Ordonnance IPAS[1671].

2220 Comme son nom l'indique, le système IPAS concerne la gestion et l'indexation de dossiers et de personnes. Sa mise en œuvre a pour but de traiter des données concernant des affaires de l'Office fédéral de la police et de gérer le suivi des dossiers. Dans ce dessein, il est composé de trois sous-systèmes: le système de traitement des données relatives à la coopération policière internationale et intercantonale, le système visant l'identification de personnes dans le cadre de poursuites pénales et de la recherche de personnes disparues, et le système de gestion des affaires et des dossiers de la Fedpol (art. 1 al. 2 O-IPAS *cum* 12, 14 et 18 LSIP).

2221 Le système IPAS permet de faciliter la gestion des documents et des dossiers qui se rapportent à des affaires impliquant des personnes physiques, des personnes morales ou des objets (art. 3 al. 2 O-IPAS). A cette fin, il comprend les catégories Interpol, Europol, N-SIS, AFIS-ADN, recherche de personnes disparues et documents d'identité (art. 3 al. 1 et 4 O-IPAS).

2222 Ainsi, il est possible de relier certaines informations au système principal ou à d'autres systèmes d'informations gérés par la Fedpol. Par exemple, nous l'avons vu, grâce au système IPAS, il est possible d'anonymiser, à l'aide d'un numéro de contrôle, un échantillon d'ADN et n'identifier le donneur qu'en cas de hit[1672].

d. Le système automatisé d'identification des empreintes digitales – AFIS

2223 Le système automatisé d'identification des empreintes digitales – AFIS – réglementé par l'Ordonnance AFIS ayant déjà fait l'objet d'une présentation lors de l'analyse de la preuve dactyloscopique[1673], nous nous limitons à rappeler l'importance de cette base dans le cadre

[1671] Ordonnance du 15 octobre 2008 sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (O-IPAS), RS 361.2.

[1672] Supra Partie II, Chapitre 2, II, A, 4, c, n° 836 ss; Supra Partie II, Chapitre 2, II, B, 1, b, ii, n° 886 ss.

[1673] Supra Partie II, Chapitre 2, I, A, 2, c, i et ii, n° 543 ss et 549 ss; Supra Partie II, Chapitre 2, I, B, 1, b, ii et iii, n° 579 ss et 590 ss.

de l'identification qui est devenue, par sa qualité et son efficacité, indissociable du paysage sécuritaire suisse et de l'identification en procédure pénale[1674].

e. La banque de données nationale sur les profils d'ADN – CODIS

2224 La banque de données nationale sur les profils d'ADN – CODIS – fondée sur la Loi sur les profils d'ADN et l'Ordonnance sur les profils d'ADN a également fait l'objet d'une analyse dans le cadre de la preuve génétique[1675]. Nous ne revenons donc pas sur le sujet, hormis pour signaler son importance croissante comme cela prévaut pour la base de données AFIS.

f. Quelques autres bases de données

2225 Nous pouvons brièvement citer deux autres bases de données qui sont essentielles dans le travail de l'autorité pénale.

2226 Le système d'information en matière de documents d'identité ISA[1676] contient essentiellement les données enregistrées sur les documents d'identité. Cette base de données est notamment utilisée pour vérifier l'identité présentée par un prévenu ou un suspect, ou pour vérifier l'authenticité des documents d'identité.

2227 La base de données VOSTRA n'est autre que le casier judiciaire informatisé (art. 1 O-VOSTRA)[1677]. Les données sont essentiellement utilisées pour la conduite de procédures pénales, l'exécution des peines et de mesures ainsi que le contrôle de sécurité (art. 3 à 7 O-VOSTRA)[1678].

[1674] Bulletin d'information AFIS Système automatique d'identification des empreintes digitales http://www.fedpol.admin.ch [consulté le 08.05.2016].

[1675] Supra Partie II, Chapitre 2, II, B, 1, a, ii, n° 850 ss; Supra Partie II, Chapitre 2, II, B, 1, b, ii, n° 886 ss; Supra Partie II, Chapitre 2, II, C, 2, n° 1030 ss.

[1676] Loi fédérale du 2 juin 2001 sur les documents d'identité des ressortissants suisses (LDI), RS 143.1.

[1677] Ordonnance fédérale du 29 février 2006 sur le casier judiciaire (O-VOSTRA), RS 331.0.

[1678] MÉTILLE, Thèse, p. 285.

3. L'utilisation des bases de données et la protection des données personnelles

a. Les atteintes à la sphère privée et à l'autodétermination informationnelle

2228 La naissance et le développement de l'informatique, sa diffusion progressive et son intégration dans le travail de la police et des autorités judiciaires ont soulevé des problèmes – notamment sur la collecte et la sécurité des données – et suscité quelques débats, notamment, sur l'ingérence aux droits fondamentaux.

2229 Les facilités et la rapidité du processus de détection ou de confirmation *via* les bases de données couplées avec la nécessité de recourir à moins de ressources humaines sur un même dossier ont immanquablement développé les recherches et traitements informatisés par la police. Ces dernières années, le nombre et la nature des bases de données gérées et exploitées par les autorités pénales s'étant accrus[1679], les atteintes à la vie privée sont devenues plus fréquentes et d'une intensité plus importante dès lors que les données recueillies s'étendent à tous les aspects de la vie publique, privée et aux informations personnelles[1680].

i. Quelles menaces pour la vie privée et les libertés fondamentales?

2230 Le traitement des informations pertinentes pour une enquête pénale et pour l'administration de la justice existe depuis longtemps. D'abord effectués manuellement, l'enregistrement et le traitement des données se sont informatisés. Les possibilités de stockage ont augmenté, la vitesse de traitement s'est accrue, l'architecture des bases de données s'est améliorée et l'utilisation a été facilitée au fur et à mesure de l'évolution dans le monde informatique.

2231 La caractéristique principale d'une base de données est de recueillir et d'enregistrer des informations généralement personnelles. Pour rappel, grâce aux traitements informatisés, il est possible de trier, de fusionner, d'effectuer des regroupements avec des informations d'une autre base de données, de sélectionner, de mettre à jour, etc. les données enregistrées dans un système[1681]. Toutes ces possibilités engendrent l'accumulation des informations. En effet, avant, le traitement manuel nécessitait de ne conserver que certaines données sans quoi le travail était impossible ou gargantuesque; aujourd'hui, si nous regroupons la totalité des

[1679] CORNU, p. 257 ; DSG-BELSER, p. 40. Supra Partie II, Chapitre 3, III, B, 2, n° 2208 ss.

[1680] CORNU, P. 257; PAOLETTI, p. 54; RIBAUX, p. 148; VITALIS, p. 137-139.

[1681] DSG-WALDMANN, OESCHGER, p. 842; VITALIS, p. 55.

données collectées dans une unique base de données, nous ne pourrions que constater qu'il est possible de nous suivre et de contrôler tous nos faits et gestes.

2232 Le simple citoyen peine parfois à se rendre compte quelles autorités, entreprises ou personnes privées détiennent des informations personnelles, mais aussi quelles sont ses données personnelles qui sont enregistrées, traitées, voire regroupées. Ainsi, l'accroissement des environnements informationnels crée le risque de perdre peu à peu la maîtrise des données qui nous concernent et de voir sa vie privée violée de manière inadmissible.

2233 La Cour européenne des droits de l'Homme[1682] et le Tribunal fédéral[1683] ont à plusieurs reprises reconnu que l'enregistrement et le traitement d'informations personnelles dans une base de données créent une ingérence au droit à l'autodétermination informationnelle (art. 8 § 1 CEDH et 13 al. 2 Cst). Il va sans dire que le regroupement des données permettant de créer des profils de la personnalité (art. 3 let. d LPD et art. 4 let. c LIPAD/GE) engendre un risque plus élevé pour le respect des garanties des droits personnels.

2234 Lors de l'analyse de la preuve dactyloscopique et celle de la preuve génétique, nous avons abordé la nature et la gravité des ingérences aux droits fondamentaux consécutives à l'emploi des bases de données AFIS et CODIS[1684]. Les informations concernant l'atteinte aux droits fondamentaux par l'utilisation de ces deux bases de données sont généralisables à toutes les bases de données exploitées par une autorité pénale.

2235 Ainsi, plus le nombre de bases de données et de recoupements entre elles augmentent, plus il y a de risque d'une ingérence disproportionnée à la vie privée, au droit à l'autodétermination informationnelle et plus le risque de violation de la présomption d'innocence est important.

[1682] CourEDH, Affaire *Leander c. Suède*, arrêt du 26 mars 1987, § 48; ComEDH, Affaire *Herbecq et l'association ligue des droit de l'Homme c. Belgique*, arrêt du 14 janvier 1998, 32200/96 et 32201/96, p. 92; CourEDH, Affaire *Amann c. Suisse*, arrêt du 16 février 2000, 27798/95, § 65; CourEDH, Affaire *Rotaru c. Roumanie*, arrêt du 4 mai 2000, 28341/95, § 43-44; CourEDH, Affaire *Khelili c. Suisse*, arrêt du 18 octobre 2011, 16188/07, § 55-56; CourEDH, Affaire *M.M c. Royaume-Uni*, arrêt du 13 novembre 2012, 24029/07, § 187-188.

[1683] ATF 120 Ia 147, 149 = JdT 1996 IV 61, 61; ATF 124 I 80, 81-82 = JdT 2000 IV 24, 25-26; ATF 128 II 259, 269 = JdT 2003 I 411, 420 = SJ 2002 I 531, 531-532; ATF 133 I 77, 80-81; ATF 137 I 167, 172-173.

[1684] Supra Partie II, Chapitre 2, I, B, 1, b, ii, n° 579 ss; Supra Partie II, Chapitre 2, I, C, 3, n° 739 ss; Supra Partie II, Chapitre 2, II, B, 1, a, ii et iii, n° 850 ss et 853 ss; Supra Partie II, Chapitre 2, II, C, 2, a, ii, n° 1040 ss; Supra Partie II, Chapitre 2, II, C, 2, c, n° 1060 ss.

ii. Comment limiter des ingérences inacceptables et les craintes suscitées par l'exploitation des bases de données?

a) Les principes généraux

2236 L'évaluation de la justification de l'ingérence causée par le traitement informatisé des bases de données AFIS et CODIS fournit un premier élément de réponse[1685].

2237 Toute exploitation d'une base de données par une autorité pénale doit reposer sur une disposition légale, être justifiée par un intérêt public prépondérant et respecter le principe de proportionnalité.

2238 La limitation à un certain cercle d'individus ou à certaines circonstances, la limitation de la conservation et la destruction des données sont des points essentiels pour reconnaître l'atteinte à l'autodétermination comme proportionnée[1686].

b) La surveillance, la transparence et l'harmonisation des procédures

2239 Trois autres points peuvent limiter les craintes suscitées par l'exploitation des bases de données et le risque d'ingérences inacceptables: la mise en place d'une surveillance drastique et complète dans la gestion des fichiers, l'obligation du respect de la transparence et l'harmonisation des dispositions liées à la constitution et à l'exploitation des données personnelles[1687].

2240 Grâce à ces éléments, les particuliers peuvent mieux appréhender le traitement des données personnelles qui les concernent et mieux comprendre la procédure applicable à la gestion des bases de données.

[1685] Supra Partie II, Chapitre 2, I, B, 1, b, ii, n° 579 ss; Supra Partie II, Chapitre 2, I, C, 3, n° 739 ss; Supra Partie II, Chapitre 2, II, B, 1, a, ii et iii, n° 850 ss et 853 ss; Supra Partie II, Chapitre 2, II, C, 2, a, ii, n° 1040 ss; Supra Partie II, Chapitre 2, II, C, 2, c, n° 1060 ss.

[1686] TF 1C_363/2014 du 13 novembre 2014, c. 2 = SJ 2015 I 128, 129-130.

[1687] BONDALLAZ, protection des personnes, p. 440, METILLE, Thèse, p. 295-300; Message, CPP, p. 1138; VITALIS, p. 144.

1. La surveillance de la gestion des bases de données

2241 La mise en place d'une surveillance doit permettre de contrôler les données qui sont enregistrées, traitées et conservées, de découvrir si des informations inutiles devant être détruites ou ne respectant pas le principe de finalité sont recueillies et conservées, et si les conditions légales pour l'exploitation et la conservation des données sont respectées.

2242 Le préposé fédéral à la protection des données personnelles et à la transparence (art. 27 LPD) et les services cantonaux compétents – le préposé à la protection des données à Genève en ce qui concerne les bases de données cantonales (art. 56 LIPAD/GE) – sont chargés de vérifier le respect des normes en vigueur.

2243 Néanmoins, vu l'ampleur de leurs tâches, il ne leur est pas possible d'avoir un œil sur toutes les données intégrées et conservées. C'est pourquoi, la surveillance n'est qu'un garde-fou qui n'empêche pas en soi les craintes de l'opinion publique sur la gestion des fichiers.

2. Le devoir d'informer

2244 Le respect du principe de transparence contient deux aspects. D'une part, il s'agit d'informer le public et, d'autre part, de leur octroyer un droit d'accès[1688].

2245 Concernant l'information, il s'agit de porter à la connaissance de la population la création d'une base de données et les informations qu'elle peut contenir. En droit fédéral et en droit cantonal genevois, un registre, respectivement un catalogue, est tenu par le préposé (art. 11a et 14 LPD et 43 LIPAD/GE)[1689]. En outre, l'organe fédéral a le devoir d'informer les personnes concernées par toute collecte de données la concernant (art. 11a et 18a LPD et 18 LIPAD/GE)[1690].

3. Le droit d'accès

2246 Il faut différencier l'exercice du droit d'accès en dehors d'une procédure pénale et le droit d'accès dans le cadre d'une telle procédure.

[1688] DSG-EPINEY, p. 544; MEIER P., p. 275.

[1689] DSG-EPINEY, FASNACHT, p. 544; MEIER P., p. 347; ROSENTHAL, JÖHRI, art. 7*a* N 11.

[1690] DSG-EPINEY, FASNACHT, p. 608; DSG-WALDMANN, BICKEL, p. 691; ROSENTHAL, JÖHRI, art. 4 N 51.

a. Le droit d'accès en dehors d'une procédure pénale

2247 L'ordonnance RIPOL, l'Ordonnance IPAS, la Loi sur les profils d'ADN et l'Ordonnance sur les profils d'ADN ne règlent pas expressément le droit d'accès aux données. En l'absence de dispositions spéciales, le droit d'accès prévu aux art. 8 et 9 LPD, soit un droit d'accès direct[1691], est applicable. D'ailleurs, la LSIP y renvoie expressément (art. 7 LSIP).

2248 Ainsi, toute personne peut demander au maître du fichier – la Fedpol – si des données la concernant sont traitées dans les systèmes automatisés RIPOL, IPAS ou CODIS.

2249 Le système JANUS a une réglementation particulière. L'accès direct est octroyé en ce qui concerne les saisies dans le système d'appui aux enquêtes de la police judiciaire (art. 2 al. 2, 3 al. 2 et 25 let. c O-JANUS *cum* art. 7 al. 4 et 10 LSIP).

2250 En revanche, l'accès est limité en ce qui concerne les données saisies dans le système informatisé des Offices centraux de police (art. 3 al. 1 et 3 et 25 let. a et b O-JANUS), exception faite des données transmises dans le cadre de la coopération avec d'autres Etats Schengen (art. 3 al. 4 et 25 let. b O-JANUS) et des données cantonales (art. 3 al. 5 et 25 let. d O-JANUS).

2251 Quant aux systèmes AFIS, il ne contient aucune disposition relative aux droits d'accès. Cette absence s'explique par le fait qu'aucune donnée nominale n'est intégrée dans cette base de données[1692].

b. Le droit d'accès dans le cadre d'une procédure pénale pendante

2252 La Loi fédérale sur la protection des données et la loi cantonale genevoise sur l'information du public, l'accès aux données et la protection des données personnelles ne s'appliquent pas aux procédures pénales pendantes (art. 2 al. 2 let. c LPD et art. 3 al. 3 let. b LIPAD).

2253 Dès lors, seul celui qui fait valoir un intérêt à la procédure – soit celui qui participe à la procédure pénale – peut bénéficier du droit de consulter le dossier (art. 101 *cum* 107 CPP).

2254 Ainsi, une personne qui ne participe pas à la procédure doit attendre sa clôture définitive pour pouvoir bénéficier du droit d'accès sur les données recueillies qui la concernent. Ce cas

[1691] A ce sujet: DSG-EPINEY, FASNACHT, p. 612-613; MEIER P., p. 370-372.

[1692] Supra Partie II, Chapitre 2, I, B, 1, b, ii, a), n° 582 ss; Supra Partie II, Chapitre 2, I, C, 3, b, n° 747 ss.

de figure est plutôt rare, les éléments du dossier de procédure concernent généralement une partie. Néanmoins, il peut se présenter. Dès lors, nous pourrions nous interroger si l'inapplicabilité générale de la LPD en cas de procédure pendante ne contrevient pas aux art. 8 § 1 CEDH et 13 al. 2 Cst.

2255 En accord avec une partie de la doctrine[1693], il nous semble préférable d'instaurer un droit d'accès même durant une procédure pénale pendante pour les non-participants, étant précisé qu'il serait possible de le limiter ou le différer en appliquant par analogie l'art. 9 LPD.

4. L'harmonisation des procédures

2256 La LPD – pour les systèmes informatisés fédéraux – et la LIPAD/GE – pour les systèmes automatisés cantonaux genevois – soumettent quelques exigences d'ordre général. Pour le surplus, la procédure diffère pour chaque base de données, dès lors qu'elles sont réglementées par des ordonnances spécifiques.

2257 L'harmonisation du droit offre une meilleure sécurité juridique. Certes, certaines dispositions doivent rester spécifiques aux diverses bases de données: leur champ d'application, leur contenu, les compétences pour gérer, avoir accès, enregistrer ou traiter des données. En revanche, il ne nous paraît pas souhaitable, notamment, que le droit d'accès des particuliers diffère d'une base de données à l'autre.

2258 Le droit d'accès est un droit primordial des particuliers dans le respect de leur vie privée et dans l'exercice de leur droit à l'autodétermination informationnelle[1694]. Il doit permettre à chacun de contrôler les autorités et de les obliger à transmettre les informations collectées à l'insu de la personne, éventuellement à corriger ou effacer des données.

2259 C'est pourquoi, dans l'idéal, les art. 8 et 9 LPD et leurs corollaires au niveau cantonal, les art. 24 et 26 LIPAD/GE, devraient être appliqués[1695]. Ainsi, les particuliers pourraient exercer leurs droits avec une meilleure aisance, compléter le contrôle des autorités effectué par le préposé fédéral et les préposés cantonaux, et, ainsi, amoindrir leur crainte du "Big Brother".

[1693] BSK-DSG-MAURER-LAMBROU, KUNZ, art. 2 N 27; ROSENTHAL, JÖHRI, art. 2 N 31-32.

[1694] BSK-DSG-GRAMIGNA, MAURER-LAMBROU, art. 8 N 1 ; MEIER P., p. 361.

[1695] A ce sujet, voir: DSG-WALDMANN, OESCHGER, p. 865 ; METILLE, Thèse, p. 305-308.

b. L'utilité des bases de données

2260 L'automatisation et la création de bases de données comprenant des données personnelles menacent certes le respect à la vie privée ainsi que toutes les libertés personnelles, mais, en contrepartie, l'influence des ordinateurs sur la société a eu un bienfait quant à la facilitation de l'enregistrement, du traitement, de l'analyse, etc. des informations.

2261 La prévention et la répression des infractions commandent que les autorités pénales puissent agir rapidement et efficacement. En disposant de renseignements détaillés, valables et actuels, il est possible de cibler les soupçons sur une ou plusieurs personnes, de confondre un auteur d'infraction ou de lier deux affaires entres elles et de bénéficier notamment de plus d'informations, voire d'indices.

2262 De manière générale en procédure pénale, la surveillance, la recherche d'indice ou de preuve et leur analyse ne sont utiles que si le but recherché – prouver un fait, identifier ou confondre l'auteur de l'infraction – peut être atteint. Pour ce faire, la récolte des informations susceptibles de prouver un fait allégué doit se poursuivre avec le traitement et l'analyse de ladite information.

2263 La croissance constante du volume de données recueillies à montrer les limites du classement manuel. La technologie du traitement automatisé de données offre la possibilité de conserver une quantité presque illimitée de données, de rechercher des informations rapidement et d'effectuer des liens qui étaient jusqu'alors impossibles ou extrêmement longs[1696].

2264 Toutes les techniques ou sciences présentées dans notre étude peuvent faire l'objet de fiches informatisées et être intégrées à une base de données. Ainsi, en enregistrant les indices dactyloscopiques, les prélèvements ADN et les données de localisation, en traitant les données de facturation, les images de vidéosurveillance, etc. et en couplant toutes les informations recueillies – moments et lieux de commission des infractions, modes opératoires, éléments pertinents, etc. –, l'autorité pénale peut développer ou gérer des hypothèses de travail.

2265 A partir des faits constatés, les informations obtenues peuvent par exemple permettre d'affirmer que deux scènes de crimes sont liées entre elles, parce que la présence d'un même individu est constatable ou simplement parce que le mode opératoire est similaire.

[1696] CORNU, p. 258; METILLE, Thèse, p. 74; RIBAUX, p. 136-137; ROSSY, p. 73.

2266 Néanmoins, les bases de données ne sont pas et ne seront jamais des "créatrices" de preuve[1697]. Elles ne font que confirmer une hypothèse issue du travail d'enquête et du raisonnement des enquêteurs, ou, si aucune hypothèse n'est préalablement formulée, elles peuvent mettre en évidence une voie possible de raisonnement en suggérant de s'intéresser à certaines données particulières.

4. La fiabilité des bases de données dans la recherche criminelle

2267 Pour offrir une assistance efficace à l'autorité pénale, un système informatisé et les données qu'il contient doivent revêtir une certaine fiabilité et qualité.

2268 La présente partie expose les risques humains ou techniques qui peuvent affaiblir la valeur des données conséquemment l'utilisation des bases de données par l'autorité pénale.

a. Les risques humains

2269 Le facteur humain est le principal facteur de risque dans l'utilisation, l'exploitation et la gestion d'une base de données.

i. L'adéquation et la qualité des données

2270 Le principe d'adéquation des données repose sur le postulat qu'une information enregistrée dans une base de données n'est utile que si elle est exacte[1698]. Ainsi, l'intégration ne doit pas être erronée et une donnée fausse ou devenue obsolète ne doit pas être conservée.

2271 La LPD et la LIPAD/GE intègrent ce principe dans leurs modalités d'exploitation des fichiers automatisés. L'art. 5 al. 1 LDP prévoit que le maître du fichier "*doit s'assurer qu[e les données] sont correctes. Il prend toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes [...]*", et l'alinéa 2 prévoit le droit de rectification par le titulaire des données. Quant à l'art. 36 al. 1 LIPAD, la disposition prévoit que "*[les] institutions publiques veillent [...] à ce que [les données personnelles] soient exactes et si nécessaire mises à jours et complétées, autant que les circonstances permettent de l'exiger.*". Cette dernière disposition prévoyant l'adéquation des données selon les circonstances, le

[1697] RIBAUX, p. 142.

[1698] ETIZONI, p. 49-51; MARTIN D., p. 26; METILLE, Thèse, p. 73.

régime juridique applicable aux bases de données cantonales est moins strict que celui applicable aux systèmes informatisés fédéraux, mais l'exactitude des données reste une préoccupation des autorités.

2272 Malgré ces dispositions, il n'est pas rare que les informations collectées soient fausses ou deviennent obsolètes. A l'appui de ce constat, nous pouvons nous référer à une étude réalisée en France. La loi française prévoit qu'"*un traitement ne peut porter que sur des données à caractère personnel [qu'à condition qu'elles soient] adéquates [...]*". Le CNIL a contrôlé, en 2009, le système de traitement des infractions constatées – STIC. Durant ce contrôle, il a été constaté que 70% des fiches nouvellement enregistrées comprenaient des erreurs et que 83% des fiches personnelles faisant l'objet d'une demande de droit d'accès étaient incorrectes[1699].

2273 La conclusion du CNIL démontre qu'un nom mal orthographié, une donnée saisie dans une mauvaise fiche, une information non confirmée ou non vérifiée s'avérant fausse, etc. ne sont pas des erreurs anodines et rares.

2274 Une inadéquation des données peut avoir des répercussions importantes sur le résultat du traitement informatisé. En effet, un nom faux ou, par exemple, l'intégration d'une empreinte digitale dans une mauvaise fiche peut fournir un hit après analyse qui amènera la suspicion d'une personne innocente.

ii. Le vol, la perte de maîtrise des informations de connexion et la malveillance des utilisateurs des bases de données

2275 La confidentialité, notamment de l'accès aux données collectées par les systèmes informatisés, est un facteur important pour assurer la sécurité des informations afin d'éviter qu'elles soient modifiées, détruites ou consultées indûment.

2276 Dans les environnements numériques, les êtres humains sont la faille la plus importante de sécurité[1700].

2277 L'ingénierie sociale, dont nous avons fait état précédemment[1701], exploite le facteur humain et la vulnérabilité dont les utilisateurs d'un système automatisé peuvent faire preuve. Afin d'éviter les pare-feux et les anti-virus, les hackers ou autres personnes malveillantes

[1699] CNIL, Conclusion du contrôle du STIC, p. 26.

[1700] BONDALLAZ, protection des personnes, p. 36; CAPRIOLI, p. 5.

[1701] Supra Partie II, Chapitre 3, III, A, 5, c, i, n° 2164.

introduisent des chevaux de Troie non pas directement, mais par l'entremise des utilisateurs autorisés.

2278 La vulnérabilité humaine est également exploitée pour simplement extirper frauduleusement un mot de passe et/ou un nom d'utilisateur. Sans parler de l'inconscience de certains employés qui notent sur un post-it collé sous le clavier, sous le tapis de souris, inscrivent dans un cahier leur mot de passe ou quittent leur place de travail sans verrouiller leur session informatique.

2279 En outre, la non-actualisation des logiciels anti-virus ou le refus d'installer une mise à jour immédiatement laisse la porte aux attaques pirates et à l'introduction de virus, de portes dérobées ou de chevaux de Troie.

2280 Tous ces éléments démontrent une nouvelle fois que le facteur humain cause des risques pour l'adéquation des données et la sécurité des systèmes informatisés et, conséquemment, réduit la valeur des résultats obtenus par le traitement des données, leur analyse et leur corrélation. C'est pourquoi la mise en œuvre d'une sécurité informatique adéquate, la mise à jour automatisée des logiciels de sécurité et la sensibilisation ainsi que la formation du personnel doivent être une priorité pour tout maître de fichier.

b. Les risques techniques

2281 Les bases de données même sécurisées ne sont pas complètement fiables. Le risque zéro n'existe pas. Toute mise en œuvre sécuritaire ou organisationnelle a son talon d'Achille. Les hackers, les pirates ou autres petits délinquants se connaissant en informatique ou ayant une connaissance spécialisée dans le domaine trouvent – généralement rapidement – comment procéder pour mettre à mal le réseau et la sécurité d'un système informatisé en utilisant leurs failles.

2282 Les bases de données étant un dispositif informatique, elles fonctionnent à l'aide d'un système d'exploitation. Ainsi, la discussion sur la vulnérabilité des systèmes d'exploitation lors de l'analyse des faiblesses des fichiers informatiques perquisitionnés s'applique par analogie aux risques techniques des bases de données[1702].

[1702] Supra Partie II, Chapitre 3, III, A, 5, c, i, n° 2164 ss.

5. Des perspectives d'avenir – Quelques orientations possibles de l'exploitation des bases de données par les autorités pénales

2283 Les indices qui découlent des diverses sciences et techniques s'intègrent nécessairement dans l'ensemble des éléments permettant d'élucider les faits et d'identifier les auteurs d'infractions. Ainsi, les bases de données, aujourd'hui déjà, améliorent considérablement l'efficacité de l'investigation criminelle grâce à l'organisation et à l'exploitation des données pertinentes.

2284 Dans la présente partie, nous désirons exposer deux potentialités des bases de données et de l'informatique dans la phase de comparaison qui ne sont pour l'heure pas exploités, mais qui mériteraient de retenir l'attention des autorités pénales à des fins identificatoires.

a. Les données biométriques comme aide à l'investigation criminelle

2285 La biométrie se constitue de diverses méthodes qui consistent à convertir les caractéristiques physiologiques – empreintes digitales, corps, visages, voix, etc. – en empreintes numériques[1703]. Grâce aux bases de données et à la numérisation des caractéristiques physiques, il est possible de faire des recoupements, notamment, avec des images capturées pas une caméra de vidéosurveillance ou le son d'une voix enregistrée lors d'une surveillance des télécommunications pour identifier un ou des auteurs.

2286 Dans le cadre de notre étude, deux techniques nous intéressent donc particulièrement: la reconnaissance faciale et la reconnaissance vocale qui ne sont pour l'heure pas ou peu exploitées par les autorités pénales.

i. La reconnaissance faciale des images de vidéosurveillance

2287 Avec la démocratisation de la vidéosurveillance, le nombre d'images ou de séquences vidéo disponibles à des fins judiciaires a explosé. Selon la qualité de l'image, leur potentiel d'exploitation s'accroît.

2288 La reconnaissance faciale se base sur la structure et la forme du visage. A l'aide d'un programme informatique, les données faciales – forme générale du visage, distances entre les yeux, le nez et la bouche, forme des yeux, de la bouche, du menton, etc. – sont calculées

[1703] CAI, biométrie, p. 10-19; CEYHAN, p. 34; PFPDT, Biométrie.

automatiquement[1704]. Une fois ces images intégrées dans la base de données, il est possible, à l'aide d'une photo ou d'une vidéo de bonne qualité, de comparer les visages et ainsi d'identifier les auteurs d'infraction.

2289 Dans le cadre d'identification des personnes ayant commis une infraction, le système d'information HOOGAN – collectant les données relatives aux personnes qui ont fait preuve d'un comportement violent lors de manifestations sportives organisées en Suisse ou à l'étranger – emploie le potentiel de la reconnaissance faciale. En effet, l'art. 10 al. 2 de l'Ordonnance sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN[1705] prévoit que les images collectées dans le système informatisé peuvent être traitées dans des systèmes électroniques de reconnaissance des personnes.

2290 Ce système a été le premier à utiliser le potentiel biométrique de la reconnaissance faciale. Dorénavant, l'Office des migrations emploie également cette méthode (art. 22 et 99 LAsi). La facilitation offerte par l'informatique devrait petit à petit et de plus en plus être intégrée dans les fichiers de police afin d'obtenir des résultats identificatoires plus fréquents et probants. Notons toutefois que la reconnaissance faciale s'apparente à un traitement de données personnelles et que des lois doivent être édictées pour permettre l'usage de cette possibilité biométrique.

ii. La reconnaissance vocale des enregistrements issus de la surveillance des télécommunications

2291 La voix en tant que caractéristique biométrique bénéficie d'une grande fiabilité identificatoire à l'aide de l'intonation et des sons émis[1706].

2292 Lors d'une surveillance des télécommunications, principalement d'écoutes des conversations, la voix est un indice important permettant, notamment, de s'assurer que l'interlocuteur est bien la personne surveillée. L'expertise en reconnaissance de locuteurs joue alors un rôle primordial[1707].

[1704] CAI, biométrie, p. 13-14.

[1705] Ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN (OMAH), RS 120.52.

[1706] MEUWLY, p. 6.

[1707] MEUWLY, p. 11.

2293 L'indice matériel obtenu par l'enregistrement vocal est converti à l'aide d'une méthode de codage analogique ou numérique et peut être comparé avec d'autres enregistrements sonores enregistrés dans une base de données.

2294 Actuellement, la qualité de la technologie de reconnaissance vocale n'est pas employée à large échelle vu son manque de maturité[1708]. Généralement, l'identification à l'aide d'autres caractéristiques biométriques est privilégiée et l'utilisation de la reconnaissance vocale est une *ultima ratio*.

2295 Néanmoins, l'empreinte vocale étant reconnue comme individuelle et l'intérêt des chercheurs se portant sur l'amélioration de la reconnaissance à l'aide des effets sonores et de l'intonation, il ne semble pas absurde d'envisager que les progrès dans cette technologie vont tôt ou tard impliquer son utilisation en science forensique à des fins identificatoires.

b. Le potentiel inexploité du mode Light out par le système automatique d'identification des empreintes digitales

2296 Jusqu'à maintenant – et peut-être pour de longues années encore –, l'expertise dactyloscopique s'effectue manuellement, la base de données dactyloscopique ne fournissant qu'une liste de candidats potentiels. L'AFIS n'est qu'un système de tri qui laisse toute latitude au dactyloscope pour fournir un résultat identificatoire[1709].

2297 Les capacités de l'outil de comparaison automatique sont plus importantes que l'usage actuel. Le système informatisé pourrait – notamment – être exploité de manière totalement automatique. En mode *light-out*, la base de données travaillerait indépendamment du concours de l'expert dactyloscope sur des identifications dites "faciles". Ainsi, le dactyloscope pourrait se consacrer au processus identificatoire plus complexe.

2298 Même si le mode *light-out* implique un gain de temps, une optimisation des ressources informatiques et une répartition favorable du personnel scientifique, des difficultés dans sa mise en œuvre doivent être prises en considérations. L'enjeu d'une telle utilisation du système AFIS est de permettre l'identification automatique. Cependant, il est notoire que les systèmes informatisés ne sont pas infaillibles.

[1708] METILLE, Thèse, p. 61; MEUWLY, p. 143.

[1709] BOCHET, p. 107; REMY, p. 91; Informations obtenues par Monsieur Axel GLAESER, Chef de division du service AFIS ADN. Supra Partie II, Chapitre 2, I, B, 1, b, ii, n° 579 ss ; Supra Partie II, Chapitre 2, I, C, 3, n° 739 ss.

2299 Ainsi, avant de pouvoir utiliser le système AFIS en mode *light-out*, il faut impérativement déterminer le taux d'erreur lors d'analyses automatiques des empreintes digitales, fixer un taux de vraisemblance devant être atteint pour qu'aucune vérification manuelle subséquente n'intervienne ainsi que de créer un algorithme de qualité définissant si oui ou non la trace indiciale peut être soumise à une décision automatique[1710].

2300 Dans l'hypothèse où un tel processus ne serait pas respecté, des risques trop importants de fausse identification ou de faux-négatif seraient à prévoir, ce qui diminuerait sensiblement la force et la valeur probatoire de la dactyloscopie.

IV. La synthèse des débats et conclusion

A. Les constatations générales

2301 De manière générale, nous constatons que les techniques sont des moyens adéquats d'aide à l'enquête, de recueil d'indices et d'éléments de preuve. Employées à bon escient, les modes de surveillance, de localisation et informatiques apportent de bons résultats pour élucider des faits ou pour identifier des auteurs sans toutefois constituer des preuves irréfutables qui se suffisent à elles-mêmes. En effet, nous l'avons largement démontré, toutes les techniques ont des failles qui les rendent vulnérables et qui diminuent quelque peu leur force probante.

2302 En outre, pour être utile, une mesure de surveillance – surveillance secrète de la correspondance par poste et télécommunication, les autres mesures de surveillance, l'observation, l'investigation secrète et la perquisition des supports informatiques – doit être ciblée afin d'éviter que le nombre de données recueillies soit tel qu'il n'est plus possible d'en faire usage efficacement. En effet, un nombre trop important de données ne permet pas un traitement adéquat, extensivement la détection des informations pertinentes.

2303 Le faible coût et l'utilisation aisée des moyens techniques renforcent leur position comme éléments probatoires, dès lors qu'ils sont facilement accessibles à l'autorité pénale et aux particuliers.

2304 Ainsi, l'avantage des moyens techniques dans le cadre de la procédure pénale n'est plus à démontrer.

[1710] Supra Partie II, Chapitre 2, I, A, 2, c, i, n° 544-548.

B. Les lacunes législatives depuis l'entrée en vigueur du Code de procédure pénale

2305 Nous pouvons regretter que le Code de procédure pénale soit parfois lacunaire pour envisager l'usage de quelques techniques nouvelles.

2306 Actuellement, par exemple, la simple utilisation d'un logiciel espion n'est pas prévue par la législation suisse, alors même que ce moyen technique est connu et usité depuis de nombreuses années.

2307 Au vu de l'exemple qui précède, l'évolution technologique ne semble pas totalement intégrée à la nouvelle procédure pénale. Il est vrai que les art. 280 ss CPP prévoient de façon générale l'utilisation "d'autres dispositifs techniques" ou que les art. 282 ss CPP ne limitent pas l'observation à des moyens techniques particuliers. Néanmoins si la problématique des logiciels espions et/ou des claviers espions se pose, nous pourrions envisager que bien d'autres technologies importantes pour les autorités pénales ne puissent être employées immédiatement à défaut de base légale justifiant l'ingérence aux droits fondamentaux.

2308 Nous pouvons également largement regretter le vide juridique causé par la mise en vigueur du Code de procédure pénale concernant l'emploi de mesure de surveillance préventive[1711]. Même si quinze cantons ont – ou sont sur le point d'avoir – une législation en la matière, d'autres comme Genève, se trouvent dépourvus partiellement de moyens d'enquête essentiels, à tout le moins jusqu'à la mise en vigueur de la nLPol, et certains cantons sont même totalement dépourvus de dispositions légales autorisant les mesures préventives.

2309 En outre, pour la sécurité juridique et afin que la population sache à quoi s'attendre d'un canton à l'autre, une harmonisation dans ce domaine serait idéale ou à tout le moins, dès lors que les législations sur la police sont du ressort des cantons, qu'un concordat intercantonal fixant des modalités générales sur le sujet soit ratifié par tous les cantons.

[1711]Supra Partie II, Chapitre 3, I, A, 2, c, i, n° 1143 ; Supra Partie II, Chapitre 3, I, A, 2, c, ii, a), n° 1149; Supra Partie II, Chapitre 3, I, A, 3, ii, n° 1242 ss; Supra Partie II, Chapitre 3, I, A, 4, c, ii, n° 1356 ss.

C. La procédure différenciée pour ordonner une mesure de surveillance, l'utilisation d'un autre dispositif technique, l'observation, l'investigation secrète et les recherches secrètes

2310 Deux points ont été relevés durant l'analyse des diverses techniques. Premièrement, les listes des infractions sur lesquelles doivent porter les soupçons ne sont pas identiques[1712]. Deuxièmement, l'autorisation n'est pas toujours exigée[1713].

2311 Le législateur justifie – généralement – les divergences de procédure selon l'ingérence et la nature de l'atteinte créées par la mesure de contrainte considérée.

2312 Néanmoins, nous avons vu que dans le cadre des moyens de localisation des divergences procédurales ne se justifient guère.

2313 Premièrement et pour des raisons historiques, le législateur a différencié la localisation à l'aide des champs d'antennes et la localisation par satellite. Alors que ces deux techniques ont la même intensité dans l'atteinte aux droits fondamentaux et qu'elles ont toutes deux pour conséquence de positionner dans l'espace et dans le temps une personne ou un objet, la localisation à l'aide d'un appareil mobile peut être ordonnée plus largement que la localisation GPS qui nécessite des soupçons sur une des infractions listées à l'art. 269 al. 2 CPP.

2314 Deuxièmement, le législateur différencie les cas d'utilisation d'autres dispositifs techniques et l'observation. La première de ces mesures de contrainte nécessite une autorisation du tribunal des mesures de contrainte, la deuxième ne requiert l'octroi d'une autorisation qu'après un mois et non pas d'une autorité judiciaire indépendante, mais du ministère public. Il est vrai que, même si globalement, une mesure de surveillance à l'aide d'un autre dispositif technique est plus intrusive dans la vie privée qu'une observation, tel n'est pas le cas dans le cadre de la localisation par GPS. En effet, contrairement à la filature qui permet de localiser et de visualiser les faits, la localisation par GPS ne fait que positionner la personne et par conséquent atteint moins gravement à la sphère privée. Il n'en reste pas

[1712] Supra Partie II, Chapitre 3, I, A, 2, a, ii, n° 1129; Supra Partie II, Chapitre 3, I, A, 2, c, ii, a) n° 1146; Supra Partie II, Chapitre 3, I, A, 4, c, i, c) n° 1348; Supra Partie II, Chapitre 3, II, C, 2, a, ii, a), n° 1754-1755; Supra Partie II, Chapitre 3, III, A, 3, c, i, b), 4 n° 2015.

[1713] Supra Partie II, Chapitre 3, I, A, 2, b, ii, n° 1138; Supra Partie II, Chapitre 3, I, A, 2, a, iv, b), n° 1173 ss; Supra Partie II, Chapitre 3, I, A, 2, a, v, d), n° 1216 et 1220; Supra Partie II, Chapitre 3, I, A, 4, c, ii, c), n° 1365; Supra Partie II, Chapitre 3, II, C, 2, a, i, d), n° 1750; Supra Partie II, Chapitre 3, III, A, 3, c, i, b), 4, n° 2010 ss; Supra Partie II, Chapitre 3, III, A, 3, c, i, c), 2, b), n° 2040 et 2044-2045.

moins que la localisation GPS est soumise aux régimes des art. 280 ss CPP, soit à des conditions d'exécution plus strictes que la filature.

2315 Ainsi, la différenciation des procédures prévues dans le cadre de mesure de surveillance technique n'est pas toujours justifiée et crée quelques incompréhensions.

TROISIEME PARTIE: LA CONCLUSION ET LES PROPOSITIONS

2316 Nous avons développé quelques disciplines que la science et la technique peuvent apporter à la recherche de preuve en procédure pénale. Le nombre de nouvelles technologies existantes et futures ne nous permet pas d'être exhaustifs.

2317 Néanmoins, les analyses réalisées nous suffisent pour répondre aux deux questions laissées en suspens à savoir: "*Sommes-nous face à une nouvelle conception du système probatoire?*" (Chapitre 1), et "*La collaboration entre les autorités pénales et les experts est-elle adéquate?*" (Chapitre 2). En parallèle des réponses apportées à ces questions, nous émettrons des critiques et des propositions afin de permettre une meilleure pesée de la valeur probatoire des nouvelles technologies, extensivement une meilleure administration de la justice.

2318 Précisons que la présente partie n'a pas pour dessein de synthétiser les caractéristiques des sciences ou des techniques analysées, d'émettre des critiques particulières à chaque mode probatoire ou encore d'effectuer des propositions spécifiques, dès lors que ces divers éléments ont fait l'objet d'écrits propres à chaque science et technique au cours de notre étude.

2319 Ainsi, la conclusion et les propositions effectuées sont générales, globales et applicables à l'appréciation de la valeur probatoire de toutes les preuves scientifiques et techniques, même futures.

CHAPITRE 1: SOMMES-NOUS FACE A UNE NOUVELLE CONCEPTION DU SYSTEME PROBATOIRE?

2320 L'utilisation délinquante des technologies et la nécessité de concourir à la bonne administration de la justice en assurant la punissabilité des auteurs d'infraction ont obligé la police, le ministère public et les tribunaux à agir. En se servant des avantages des sciences et des techniques, ils se sont procurés des nouveaux moyens d'investigation.

2321 En outre, il n'est plus utile de démontrer que, grâce aux nouvelles technologies, les autorités pénales bénéficient de moyens probatoires importants qui sont largement appréciés au vu de leur prétendue objectivité, les juristes omettant bien souvant que ces preuves matérielles nécessitent d'être interprétées, voire analysées et traitées par des experts.

2322 Ce constat, démontré tout au long de notre travail, nous amène à nous demander si les preuves issues des nouvelles technologies ne constituent dorénavant pas une matérialisation de la réalité qui équivaudrait à l'aveu ou au jugement de Dieu ayant cours respectivement dans le système procédural inquisitoire et le système procédural accusatoire.

2323 Après avoir établi que la valeur probante des preuves scientifiques ou techniques n'est pas toujours analysée *in concreto* (I.), nous verrons la problématique de la stratégie du doute utilisée par la défense dans le procès pénal (II.), et l'impact que ces divers éléments ont sur l'intime conviction du juge et sa liberté d'appréciation des preuves (III.).

I. L'importance des preuves scientifiques ou techniques

2324 Depuis l'introduction, en 1829, du système de la preuve morale effaçant les abus de la preuve légale, il semble que ce régime soit indiscuté et indiscutable[1714]. Néanmoins, l'introduction des preuves scientifiques et techniques nous laisse entrevoir un léger retour vers la preuve légale[1715].

[1714] Supra Partie I, Chapitre 1, II, A, 3, b, n° 63 ss.

[1715] Supra Partie I, Chapitre 1, II, A, 2, b, n° 49 ss.

A. La reconnaissance des nouvelles technologies comme preuve de la vérité

2325 Nous vivons actuellement dans un monde que nous pourrions caractériser de technologique. Autant les instruments informatiques, que les sciences forensiques ou les techniques matérielles fascinent l'opinion publique par leur objectivité et leur possibilité d'établir les faits ou d'identifier les auteurs. L'avis et la reconnaissance du *quidam* pour la crédibilité des nouvelles technologies n'a pas manqué d'intéresser la justice.

2326 En procédure pénale, grâce à leur nature physique, à la matérialisation qu'elles apportent et au degré de précision ressortant des indices scientifiques ou techniques, les nouvelles technologies ont une place privilégiée. Elles sont considérées comme des moyens de preuves plus fiables et certains que toutes autres formes d'indices ou d'éléments probatoires. Certains auteurs de doctrine décrivent même les moyens de preuves scientifiques ou techniques comme une arme absolue dont le juge use et abuse pour faire triompher la vérité.

2327 En outre, la communauté mondiale et certains juristes n'hésitent pas à soutenir que les indices scientifiques ou techniques sont la clé pour l'issue de tout procès pénal[1716].

B. L'administration des nouvelles technologies et l'appréciation de la preuve

2328 Avec certitude, nous pouvons affirmer que l'aveu n'est plus la reine des preuves. Mais qu'en est-il des preuves matérielles et objectives issues des nouvelles technologies?

2329 Le système des preuves morales qui a cours actuellement dans notre système procédural impose de ne pas quantifier la valeur probante par avance.

2330 Néanmoins, l'idéologie et la croyance qu'une preuve scientifique ou technique démontre la réalité de manière quasiment infaillible poussent régulièrement le juge ou les parties à administrer ces preuves sans débattre de leur valeur.

[1716] Supra Partie II, Chapitre 2, I, C, 1, b, iv, n° 708-709; Supra Partie II, Chapitre 2, II, C, 1, a, i, n° 942 ss; Supra Partie II, Chapitre 3, I, A, 4, a, i, n° 1254 ss; Supra Partie II, Chapitre 3, I, B, 4, a, n° 1587 ss; Supra Partie II, Chapitre 3, II, E, 1, a, n° 1784 ss.

2331 Hiérarchiquement, nous ne pouvons pas constater de reconnaissance probatoire plus ou moins importante en fonction des divers moyens de preuves technologiques. En revanche, les juristes – en reconnaissant un peu rapidement que ces éléments probatoires sont purement objectifs – ont tendance à les privilégier aux preuves indirectes[1717]. En effet, ils estiment que ces moyens de preuves ont l'avantage de ne pas pouvoir mentir contrairement aux témoins, aux personnes appelées à donner des renseignements ou au prévenu.

2332 L'objectivité de la preuve technologique, la matérialisation de la démonstration probatoire et le manque de connaissances des juristes pour apprécier l'élément probatoire poussent régulièrement le juge à s'en remettre à la valeur abstraite scientifique ou technique sans apprécier la preuve dans son contexte juridique.

2333 Ce premier constat nous permet déjà de démontrer que l'élément principal de la preuve morale, à savoir la libre appréciation des preuves par le juge, n'a plus réellement cours lors de l'administration d'une preuve issue des nouvelles technologies.

II. La stratégie du doute ou la décrédibilisation des preuves scientifiques ou techniques

2334 Si le juge n'a pas les connaissances scientifiques ou techniques suffisantes pour apprécier adéquatement la valeur probante des nouvelles technologies, il n'est pas non plus en mesure de déterminer avec précision les conséquences de certains risques sur la fiabilité et la crédibilité de ces mêmes éléments de preuve.

2335 La défense ne manque pas de s'appuyer sur le manque de connaissances des juges concernant les nouvelles technologies pour défendre son client et éviter qu'une preuve technologique soit jugée irréfutable.

2336 Afin de neutraliser les hypothèses issues des nouvelles technologies, les avocats se sont intéressés aux sciences et aux techniques. Plus particulièrement, ils ont recherché les failles et les risques permettant de décrédibiliser les preuves scientifiques et techniques.

[1717] Supra Partie II, Chapitre 2, I, C, 1, b, iv, n° 709-710; Supra Partie II, Chapitre 2, II, C, 1, a, i, n° 944 ss; Supra Partie II, Chapitre 3, I, A, 4, a, i, n° 1257 ss; Supra Partie II, Chapitre 3, I, B, 4, a, n° 1596 ss; Supra Partie II, Chapitre 3, II, E, 1, a, n° 1793 ss.

2337 Une preuve n'a de réelle force probante que si elle est authentique, véridique ou s'il est possible de déterminer les conséquences sur la démonstration probatoire qu'un risque ou qu'une imprécision peut avoir.

2338 Ainsi, face à une preuve matérielle, comme celle issue des nouvelles technologies, la défense tente de démontrer systématiquement que rien ne peut prouver qu'aucune modification, manipulation ou contamination n'a eu lieu.

2339 En mettant en cause la validité des preuves scientifiques ou techniques, les avocats de la défense emploient la stratégie du doute. S'il est rare de pouvoir démontrer qu'une atteinte à l'authenticité de la preuve ou à son objectivité existe réellement, il est relativement aisé de former un doute dans l'esprit du juge quant à la fiabilité de la preuve.

2340 Corrélativement à la difficulté de comprendre et d'apprécier une preuve par manque de connaissances scientifiques ou techniques, le juge qui se trouve face à une décrédibilisation de la preuve par la défense peine à pouvoir juger du réel impact de la faille ou du risque présenté. Il se voit alors obligé d'écarter la preuve scientifique ou technique apportée ou, à tout du moins, de limiter considérablement sa force probante.

2341 Ce deuxième constat renforce notre première conclusion, à savoir qu'à défaut de libre appréciation de la preuve par le juge, le système de preuve morale a évolué.

III. L'impact des preuves issues des nouvelles technologies et de la stratégie du doute sur la décision du juge

2342 L'administration des preuves semble dorénavant orientée vers un régime de semi-preuve légale où le juge n'est plus à même de s'en remettre à son impression personnelle, soit à son intime conviction. Consciemment ou inconsciemment, à défaut d'avoir l'aptitude et les capacités scientifiques ou techniques pour comprendre toutes les subtilités des preuves issues des nouvelles technologies, le juge se réfère bien souvent à l'avis de l'expert, à la fiabilité théorique du mode probatoire et à la reconnaissance scientifique des sciences ou techniques administrées.

2343 De surcroît, le manque de connaissances des magistrats dans le domaine des technologies implique également l'incapacité de ceux-ci à pouvoir déterminer si les dires de la défense adoptant la stratégie du doute sont crédibles, et quelles en seraient les conséquences pour la valeur probante.

2344 Bien entendu, pour l'aider dans sa tâche, le juge peut toujours recourir à un expert afin de lui expliquer les arguments de la défense ou de l'accusation, de lui fournir un avis spécialisé sur une preuve scientifique ou technique ou de l'informer sur les conséquences qu'un risque déterminé peut avoir sur le résultat scientifique ou technique.

2345 Cependant, cette situation ne résout pas la problématique des difficultés du magistrat à apprécier la valeur probante. En effet, en recourant à un expert pour l'aider à interpréter la valeur des nouvelles technologies, le juge entre dans un cercle vicieux où le recours à un expert est un passage obligé impliquant que la décision sur la valeur probante ne lui appartient pas à défaut de connaissances suffisantes.

2346 Par conséquent, en l'absence d'évaluation concrète et d'appréciation libre des preuves administrées, nous pouvons admettre que la valeur probante des indices scientifiques et techniques est fixée par la reconnaissance théorique dans le domaine considéré. A défaut de quantification au cas par cas de la valeur probante d'un élément probatoire, l'un des principes essentiels du système des preuves morales n'est plus respecté.

2347 Cependant, il ne s'agit pour autant pas d'un retour de la preuve légale. En effet, la valeur probatoire n'est pas fixée dans une loi, mais ressort des considérants techniques ou scientifiques. C'est pourquoi, à notre avis, la preuve scientifique peut, à l'heure actuelle, être considérée comme une semi-preuve légale, soit à mi-chemin entre une preuve morale et une preuve légale.

2348 Afin d'éviter la surévaluation des preuves issues des nouvelles technologies ou leur décrédibilisation – parfois – injustifiée, le juge doit pouvoir appréhender la valeur criminalistique des indices scientifiques et techniques. Pour éviter la perte du pouvoir décisionnel du juge et de sa libre appréciation des preuves – nous le verrons plus précisément dans le second chapitre –, il est indispensable de former les magistrats sur les sciences et les techniques exploitées en procédure pénale.

CHAPITRE 2: LA COLLABORATION ENTRE LES AUTORITES PENALES ET LES EXPERTS EST-ELLE ADEQUATE?

I. La confiance des juristes portée aux experts

A. Le principe de confiance

2349 Tout au long de notre travail, nous avons pu constater que les sciences et les techniques demandent des connaissances spécifiques dans le domaine considéré.

2350 Que ce soit au stade de l'instruction ou de la juridiction de jugement, les magistrats se trouvent dans l'obligation de recourir aux expertises. Par ailleurs, la police technique ou scientifique est fréquemment sollicitée lors des enquêtes policières. Il en résulte que le nombre de missions d'expertises judiciaires est en constante augmentation et que l'expert devient un acteur fondamental et récurrent du procès pénal.

2351 Nous l'avons également déjà exprimé, les juristes ont une grande confiance dans les experts – indépendants et impartiaux – et dans la valeur des expertises.

2352 Cette confiance apparaît dans le travail du magistrat qui ne pose guère de questions aux spécialistes, ne s'attarde que sur les résultats ou conclusions de l'expertise et ne débat pas de la force probante des sciences ou techniques.

B. Les bases de la confiance

2353 Plusieurs raisons expliquent la confiance portée aux experts lorsqu'une preuve scientifique ou technique est administrée.

1. L'impartialité et l'indépendance des experts

2354 Un expert n'est pas nommé au hasard et sans cadre juridique. Contrairement aux témoins, aux personnes appelées à donner des renseignements ou au prévenu, les experts judiciaires n'ont aucun parti pris et sont indépendants tant des parties que du juge.

2355 En outre, leur professionnalisme fonde également la confiance. En effet, ils suivent – en règle générale – des protocoles qui assurent aux juges que l'expertise a été réalisée dans les règles de l'art.

2. L'accréditation des laboratoires et l'expérience des experts

2356 Dans certains domaines, notamment pour les analyses génétiques, la Confédération et les cantons ont utilisé la possibilité offerte par le Code de procédure pénale en accréditant des laboratoires au sein desquels des experts officiels peuvent être nommés (art. 183 al. 2 CPP).

2357 L'accréditation officielle des laboratoires de médecine légale garantit un certain niveau de qualité des laboratoires et de formation des experts.

2358 En outre, nous l'avons énoncé, l'expérience des experts joue un rôle fondamental dans l'esprit du magistrat. En effet, la crédibilité d'une expertise dépend étroitement des connaissances de son rédacteur. Ainsi, la formation continue des experts et leurs années de pratique permettent d'acquérir des connaissances supplémentaires renforçant leur crédibilité.

3. La reconnaissance technique et scientifique

2359 L'art. 139 al. 1 CPP spécifie que: "*les autorités pénales mettent en œuvre tous les moyens de preuves licites qui, selon l'état des connaissances scientifiques et l'expérience, sont propres à établir la vérité.*". La lettre de la loi est claire, une nouvelle technologie n'est une preuve viable que si elle est scientifiquement ou techniquement probante.

2360 Ainsi, la confiance des juristes pour les preuves issues des nouvelles technologies est en premier lieu basée sur la reconnaissance scientifique ou technique de leur qualité identificatoire ou d'élucidation des faits.

C. Le manque de connaissances scientifiques ou techniques des magistrats

2361 Le manque de connaissances des magistrats dans les domaines scientifiques ou techniques est inhérent au principe de l'expertise, extensivement de la confiance portée aux dires de l'expert.

2362 En vertu de l'art. 182 CPP: "*Le ministère public et les tribunaux ont recours à un ou plusieurs experts lorsqu'ils ne disposent pas des connaissances et des capacités nécessaires pour constater ou juger un état de fait.*". A défaut de pouvoir analyser la preuve scientifique ou technique administrée au procès, le juge recourt aux experts. Extensivement, nous discernons difficilement comment le juge peut se positionner de manière certaine ou critiquer le rapport d'expertise.

2363 Le juge ne pouvant s'écarter que pour de justes motifs des rapports d'expertises, l'absence de compétences en matière scientifique et technique le pousse à croire en l'expert et en ses capacités à juger la force probante d'un indice.

II. Le manque d'interprétation renforçant le rôle de l'expert

2364 Actuellement, nous pouvons conclure que l'appréciation des preuves issues des nouvelles technologies ne repose que sur la confiance accordée aux rapports d'expertise.

2365 Les magistrats savent que des questions sur la crédibilité des preuves scientifiques ou techniques se posent. Ils sont également conscients qu'un examen critique selon le cas d'espèce doit être réalisé. Néanmoins, par manque de connaissance et de dialogue avec l'expert, ils ne sont pas disposés à apprécier librement les preuves apportées et sont obligés de se référer à l'avis des experts.

2366 Alors que l'expert ne devrait être désigné que pour assister le tribunal en lui fournissant des avis éclairés, il nous semble correct d'affirmer qu'il a en partie la décision juridique entre ses mains. En effet, en affirmant ou infirmant la valeur d'une démonstration scientifique ou technique, l'expert a la possibilité de faire pencher le juge en faveur ou en défaveur de l'accusation.

2367 Ce constat est renforcé par le manque cruel de questions posées à l'expert par le juge au cours des procès pénaux. En outre, lorsque des débats ont lieu ou que quelques questions sont posées, les experts peinent à exprimer clairement et simplement des considérants scientifiques et techniques. Ils oublient bien souvent que le juge n'est pas un spécialiste du domaine.

2368 Par conséquent, à l'heure actuelle, la collaboration entre les autorités pénales et les experts n'est ni suffisante, ni adéquate.

III. Les propositions

2369 Dans le dessein d'améliorer l'administration de la justice et de ne pas reconnaître un rôle de décideur à l'expert, la décision juridique sur l'admission et sur l'appréciation d'une preuve scientifique ou technique doit impliquer une réflexion conjointe des acteurs du procès pénal.

2370 Pour remplir cet objectif, il est essentiel d'améliorer la collaboration et les échanges entre les autorités pénales et les experts et, pour ce faire, une formation adéquate de ces acteurs est nécessaire.

A. La formation des juristes

2371 A la lumière des constats effectués, la formation des juristes dans le domaine des nouvelles technologies et de l'appréciation de la preuve est insuffisante. En effet, les juristes ne bénéficient pas de connaissances adéquates pour déterminer la valeur scientifique d'une preuve et pour l'interpréter à la lumière du cas d'espèce.

2372 Il ne s'agit pas ici de demander aux autorités pénales et aux juristes de devenir des experts en matière de nouvelles technologies, mais uniquement de leur inculquer quelques bases essentielles. Il faut notamment leur expliciter les problématiques et risques pouvant exister lors du prélèvement, du relever, de l'analyse, du traitement etc. de la preuve, leur fournir les éléments utiles pour apprécier un rapport d'expertise avec un œil critique et le comprendre, leur donner les outils nécessaires pour comprendre les faits établis par les éléments probatoires scientifiques ou techniques, expliciter comment des recoupements peuvent se faire entre divers indices technologiques, etc.; en d'autres termes, leur offrir la possibilité de comprendre les sciences, les techniques et les risques liés à leur usage quant à leur valeur probatoire.

2373 A noter que cette formation peut tout autant se dérouler durant les études de droit ou être une formation continue des juristes.

B. La formation des experts au monde judiciaire et au vocabulaire des juristes

2374 Les notions scientifiques et techniques étant abstraites pour un juriste, voire incompréhensibles, il faut se demander si les experts n'ont pas une part de responsabilité dans le manque d'appréciation d'un élément probatoire scientifique ou technique.

2375 Comme les juristes, les médecins, les chimistes, les physiciens ou encore les informaticiens ont tous ce que nous nommons communément une déformation professionnelle. Lorsqu'ils formulent un élément, un fait ou une explication en rapport avec leur domaine d'activités, ils ont tendance à employer les termes spécifiques à leur domaine et à aller droit au but sans explication. Dès lors, pour le simple *quidam*, il est difficile de comprendre et de critiquer les dires exposés.

2376 Une formation juridique sur ce qu'est une expertise judiciaire et ce qu'elle implique doit permettre aux experts de comprendre la place qui est la leur durant un procès pénal. Ainsi, il est essentiel que les experts aient connaissance de leurs droits et devoirs lorsqu'ils viennent en aide à la justice, et qu'ils les comprennent.

2377 En outre, une formation juridique adéquate des experts doit leur permettre de mieux cibler les éléments nécessaires à l'appréciation des preuves et de les exposer aisément. Ajoutons encore que pour parfaire la formation des experts, il est envisageable de leur donner des cours durant lesquels ils apprennent à formuler clairement, précisément et avec un vocabulaire simple leur résultat d'expertise.

C. L'amélioration de la communication entre les autorités pénales et les experts

2378 Au cours du procès pénal, l'expert se définit comme la personne qui fournit les éléments pertinents au juge pour comprendre et apprécier des éléments théoriques spécifiques.

2379 La formation des juristes dans le domaine des nouvelles technologies et la formation des experts dans le domaine juridique de l'expertise judicaire doit permettre une meilleure communication entre ces deux acteurs essentiels à la procédure pénale.

2380 Ainsi, grâce à leur formation respective, le juge doit pouvoir avoir les bases suffisantes pour critiquer un rapport d'expertise, pouvoir s'y référer à sa juste valeur et également pouvoir déterminer la crédibilité ou la fiabilité d'un élément probatoire technique ou scientifique.

2381 En outre, l'expert comprenant mieux son rôle et pouvant compter sur un minimum de connaissances acquises par les juristes, il peut expliquer de manière appropriée la démonstration apportée par l'indice issue des nouvelles technologies.

2382 Ajoutons que des rencontres et/ou séminaires conjoints – technico-juridiques – devraient également permettre de favoriser les échanges d'informations et la communication entre les autorités pénales et les experts.

LA CONCLUSION FINALE

2383 La mise en cause et la condamnation d'un individu comme auteur d'infraction constituent des actes suffisamment graves pour que des dispositifs formels ne dictent pas la décision du juge.

2384 Actuellement, nous regrettons l'orientation que semble prendre le système probatoire en procédure pénale et le rôle que tient l'expert dans cette procédure. Il paraît donc essentiel d'objectiver la preuve pénale et, pour ce faire, de former les experts et les juges afin d'obtenir une meilleure collaboration.

2385 En outre, les juristes doivent garder à l'esprit qu'une preuve – quelle qu'elle soit – est une aide ou un indice, mais ne permet en aucun cas d'assurer aux autorités policières, au ministère public ou au juge que les événements se sont effectivement déroulés comme elle le démontre ou que le prévenu est l'auteur de l'infraction. Elle ne dispense pas et ne dispensera jamais les autorités pénales à recourir à des investigations poussées pour confirmer ou infirmer sa démonstration matérielle, scientifique ou technique.

2386 Les potentiels et les risques que nous avons relevés pour chaque science ou technique traitée ne sont que des éléments pour permettre aux juristes de mieux cerner les problématiques liées à l'appréciation des preuves techniques. Les considérations qui précèdent ne sont en revanche pas des règles d'interprétation à suivre aveuglément.

2387 Ainsi, il n'existe aucun moyen infaillible pour parvenir à la vérité, ni de règles générales et abstraites pour juger de la valeur probatoire d'un indice scientifique ou technique. Chaque preuve doit être administrée, jugée et analysée dans le cas concret de l'affaire en cause.

2388 Le seul maître mot qui doit dicter l'appréciation des preuves est qu'il ne faut pas tomber dans le piège du recours systématique aux preuves scientifiques ou techniques, ou de croire qu'elles peuvent être considérées comme la *reine des preuves*. Même si leur objectivité est avérée, des failles, des risques ou des erreurs d'interprétation ne sont pas exclus, amoindrissant leur valeur et leur authenticité.

2389 Nous conclurons donc sur ces quelques mots: "Un indice matériel ne peut pas se tromper, il ne peut se dénier lui-même, [...]. Seule l'erreur humaine dans sa recherche, son exploitation et son interprétation peut diminuer sa valeur."[1718]. Médiate ou immédiate, objective ou

[1718] Paul Leland KIRK dans GALLUSER, p. 35.

subjective, matérielle ou indirecte, une preuve demande toujours une interprétation pour être administrée. Par conséquent, sa valeur probatoire doit toujours être appréciée.

GLOSSAIRES

La dactyloscopie

ARC: L'arc ou la figure adeltique correspond à une ligne papillaire allant d'une extrémité distale à l'autre de la pulpe du doigt avec en son centre une bosse sans noyau ni delta pour la forme simple et un noyau mais pas de delta pour l'arc en tente.

A noter qu'en ce qui concerne l'empreinte palmaire, la forme d'arc peut contenir un delta.

BIDELTE: Dessin papillaire contenant deux deltas.

BOUCLE: La boucle se dessine autour d'un noyau et se compose d'un delta. Il peut s'agir de boucle à droite dont les lignes proviennent de la droite et dont le delta se situe en bas à gauche du noyau, ou de boucle à gauche qui sont en miroir comparées aux premières.

A noter qu'en ce qui concerne l'empreinte palmaire, la forme en boucle peut ne contenir aucun delta.

COMPOSITE: Cette forme est une combinaison des grandes classes de dessins papillaires (arc, boucle et verticille) et se compose de deux ou de plusieurs deltas. En d'autres termes, il s'agit d'un point de confluence de trois groupes de crêtes.

DELTA: Il s'agit du point de confluence des stries provenant de la zone centrale (centre), basale (partie basse) et marginale (côtés) du dessin papillaire. Il est triangulaire et se trouve en bas à droite et/ou à gauche du noyau.

DERMATOGLYPHE: Ce terme désigne les dessins sis à la surface de la paume des mains, des doigts ou de la voûte plantaire. Ils sont constitués de crêtes, de sillons et de pli du derme.

EMPREINTE LATENTE: Les empreintes latentes sont invisibles ou difficilement détectables à la lumière directe.

EMPREINTE MOULÉE: Les empreintes moulées s'impriment sur une surface malléable, comme la cire, du mastique, de la peinture fraîche, etc.

EMPREINTE VISIBLE: Lorsqu'il existe un contraste entre la trace papillaire et le support sans traitement particulier, l'empreinte est dite visible. Elle est négative lorsque les crêtes papillaires ôtent de la suie ou de la poussière sur le support, et positive si les crêtes papillaires sont contaminées par une substance colorée comme l'encre ou le sang.

GLANDES APOCRINES: Les glandes apocrines sécrètent la sueur. Elles sont présentes dans la région anale et génitale ainsi que sous les aisselles.

GLANDES ECCRINES: Les glandes éccrines sécrètent la sueur. Elles sont plus nombreuses que les glandes apocrines. Elles se situent majoritairement à la paume des mains et à la plante des pieds.

GLANDES SÉBACÉES: Les glandes sébacées sont situées dans l'épiderme. Elles sécrètent le sébum (corps gras).

MINUTIES: Les minuties sont des points caractéristiques servant à comparer les empreintes papillaires et formées par une modification nette d'une ligne papillaire (arrêt, bifurcations ou formations de lacs, d'îlots ou d'yeux).

MONODELTE: Dessin papillaire contenant un delta.

MORPHOGÉNÈSE: La morphogénèse correspond à l'étape d'évolution d'un organisme vivant au cours de l'embryogénèse. Elle constitue l'ensemble des lois qui déterminent la structure des tissus, des organes, etc. et leur forme.

NOYAU: Le noyau est le point inférieur situé au milieu de l'empreinte où les lignes papillaires arrivent, convergent ou retournent. Il sert de repère pour situer les autres minuties, notamment le ou les deltas.

RIDGE COUNTING: La ligne comptée est une sous-division du motif en boucle. Il s'agit du résultat obtenu après le comptage des lignes papillaires sises entre le noyau et le ou les deltas.

RIDGE TRACING: La ligne tracée n'existe qu'en lien avec une figure bi- ou multideltes. Il suffit d'analyser la ligne tracée ou la ligne inférieure entre le delta gauche et le delta droit. Cette ligne peut s'approcher du delta droit par le haut, le bas ou entrer en contact.

VERTICILLIE: Le verticille se caractérise par une forme en spirale autour d'un noyau et se compose de deux deltas. Ils existent de nombreuses formes de verticilles: circulaires, ovoïdes, en spirales de droite à gauche et inversement, en besace, ou encore contenant des boucles jumelées, voire des verticilles en Z ou en S.

L'acide désoxyribonucléique

ADN VIRAL: L'ADN viral correspond à l'ADN qui compose le matériel génétique des virus.

CELLULE EUCARYOTE: Les cellules eucaryotes possèdent toutes un noyau qui contient de l'ADN.

ELECTROPHORÈSE: L'électrophorèse est une technique de laboratoire employant le champ électrique qui permet de séparer les protéines des acides nucléiques grâce à la différence de masse.

GÉNOME: Le génome est l'ensemble du matériel génétique de l'individu codé dans son ADN. Il contient des séquences codantes (transcrites en ARNm et traduites en protéines) et non-codantes (non transcrites ou transcrites en ARNm mais non traduites).

HÉMATIE: Une hématie est un globule rouge du sang. Elle ne contient pas de noyau et donc pas d'ADN.

HIT: Le terme *hit* se définit comme la correspondance entre une trace découverte sur le lieu d'un crime et le profil d'un individu fiché ou entre deux traces.

JUMEAUX HOMOZYGOTES: Les jumeaux homozygotes sont appelés communément les vrais jumeaux. Ils sont issus du même œuf qui est divisé après la fécondation.

LEUCOCYTE: Les leucocytes sont présents dans le sang, la lymphe, les organes lymphoïdes et certains tissus conjonctifs. Ils correspondent à la couche intermédiaire blanche lors de la centrifugation d'échantillons sanguins. Ils jouent un rôle important dans les défenses immunitaires.

LOCUS/LOCI: Le *locus*, au pluriel *loci*, est l'emplacement précis d'un gène sur un chromosome.

Les techniques de surveillance

CHEVAL DE TROIE: Le cheval de Troie est un logiciel d'apparence légitime conçu pour exécuter des actions à l'insu de l'utilisateur de l'appareil informatique. Ce terme désigne actuellement tout programme installé de manière frauduleuse sur un ordinateur ou tout autre appareil électronique.

GOWARE: Voir *Cheval de Troie*

IMEI: Le numéro IMEI est composé de 15 chiffres. Il permet d'identifier le téléphone mobile. Il est automatiquement transmis par le téléphone à l'opérateur téléphonique *via* le réseau.

IMSI: Le numéro IMSI est un numéro unique qui permet au réseau GSM ou UMTS d'identifier l'usager. Ce numéro n'appartient pas à l'appareil, contrairement au numéro IMEI, mais à la carte SIM employée par l'usager. Il n'est normalement pas connu de l'utilisateur.

ISDN: ISDN signifiant Integrated Services Digital Network est une architecture réseaux permettant d'associer la voix, vidéo, données et autres applications ou services.

Les techniques de localisation

ANTENNES RELAIS: Les antennes relais permettent d'émettre, de recevoir et de transporter des ondes. En d'autres termes, elles offrent la

possibilité à un appareil de téléphonie mobile de pouvoir communiquer.

BTS: Voir antenne relais

RADIOFRÉQUENCE: La radiofréquence correspond à la fréquence des ondes radioélectriques. Elle est notamment utilisée en télécommunications pour réceptionner le signal et se connecter au réseau.

Les techniques informatiques:

BLOG: Un blog est l'abréviation de *weblog"* qui se traduit généralement par "journal sur Internet". Il s'agit communément de page internet personnel ou d'espace individuel d'expression ou la parole est librement donnée aux internautes.

CARTE RÉSEAU: La carte réseau permet la connexion d'un appareil électronique au réseau.

COOKIE: Un cookie est un fichier texte enregistré sur le disque dur de l'ordinateur à la demande du serveur gérant un site internet visité. Il contient les informations sur la navigation réalisée et sert à reprendre les préférences choisies par l'utilisateur lors de sa visite.

PAQUET DE DONNÉES: Un paquet de données est une suite de données organisées permettant de constituer une unité transmise par un système de communication.

PEER-TO-PEER: Le Peer-to-Peer traduisible "d'égal à égal" en français est un type de connexion réseau par laquelle deux appareils électroniques communiquent entre eux afin de partager des fichiers stockés sur le disque dur des machines.

ROUTEUR: Le routeur est un élément intermédiaire dans un réseau informatique. Il permet de faire transiter des paquets de données d'une interface réseau vers une autre interface réseau.

TEMPORAIRE INTERNET: Les temporaires Internet ou Temp sont des fichiers dont le contenu nécessaire durant un très bref laps de temps. Lors de chaque navigation sur Internet, des fichiers temporaires sont automatiquement créés comme mémoire cache des pages internet visitées pour être affichées plus rapidement à la prochaine visite.

BIBLIOGRAPHIE

Ouvrages

AELLEN Laurence, HAINARD Frédéric, Secret professionnel et surveillance des télécommunications, *Jusletter* 23 mars 2009, n° 2.

AESCHLIMANN Jürg, *Einführung in das Strafprozessrecht: die neuen bernischen Gesetze*, Berne – Stuttgart – Vienne 1997.

ALBERTINI Gianfranco, *Die polizeilichen Massnahmen gemäss Art. 9-22 des Polizeigesetzes des Kantons Graubünden vom 20. Oktober 2004 = Le misure di polizia giusta gli art. 9-22 della Legge sulla polizia del Cantone dei Grigioni del 20 ottobre 2004*, Coire 2005.

ALBERTINI Gianfranco, FEHR Bruno, VOSER Beat (éd.), *Polizeiliche Ermittlung – Ein Handbuch der Vereinigung der Schweizerischen Kriminalpolizeichefs zum polizeilichen Ermittlungsverfahren gemäss der Schweizerischen Strafprozessordnung*, Zurich 2008 (Cité: Polizeiliche Ermittlung-NOM).

ALLMAN David, POUNDS Anthony C., *The sequence of reagents to be used to develop fingerprints at a scene of crime*, Paris 2006.

ALTENDORFER Reinhold, *Rechtsprobleme der DNA-Analyse im Strafverfahren*, Munich 2001.

AMADÒ Flavio, MOLO Giovanni, Das Verbot von "Fishing Expeditions" gemäss der Entscheidung des Bundesverwaltungsgerichts vom 5. März 2009 und den OECD-Standards, *AJP/PJA* 2009 p. 539-550.

AMEZIANE Nedjma, BOGARD Marc, LAMORIL Jérôme, *Principes de biologie moléculaire en biologie clinique*, Aldermaston 1992 (avec autorisation du Forensic Science Service).

ANCEL Hervé, La preuve biologique, in Giudicelli-Delage Geneviève (éd.), *Les transformations de l'administration de la preuve pénale: perspectives comparées*, Paris 1997, p. 139-222.

ANDRÉANI Ariane, *Le GPS: une révolution*, Boussy-Saint-Antoine 2001.

ANTOGNINI Caterina, L'appréciation des expertises scientifiques, *Jusletter* 6 juin 2011, n° 1.

ARIOLI Martina, THALMANN André, Einsatz von RFID im Rechtsverkehr, *AJP/PJA* 2006 p. 549-560.

ASHBAUGH David R., *Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology*, Colombie-Britannique 1999.

ASSOCIATION SOURIEZ-VOUS ÊTES FILMÉ, *La télésurveillance en question*, Paris, disponible sur: http://www.souriez.info/ [consulté le 08.05.2016].

AUBERT Jean-François, Notion et fonctions de la Constitutions, in Thürer Daniel, Aubert Jean-François, Müller Jörg Paul (éd.), *Verfassungsrecht der Schweiz – Droit constitutionnel suisse*, Zurich 2001, p. 3-16.

AUBERT Jean-François, MAHON Pascal, *Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999*, Zurich – Bâle – Genève 2003.

AUER Andreas, FLÜCKIGER Alexandre, La vidéosurveillance dans l'oeil de la Constitution, *AJP/PJA* 2006 p. 924-942.

AUER Andreas, HOTTELIER Michel, MALINVERNI Giorgio, *Droit constitutionnel suisse: L'Etat*, vol. I, 3ème éd., Berne 2013 (cité: AUER, HOTTELIER, MALINVERNI, Vol. I).

AUER Andreas, HOTTELIER Michel, MALINVERNI Giorgio, *Droit constitutionnel suisse: Les droits fondamentaux*, vol. II, 3ème éd., Berne 2013 (cité: AUER, HOTTELIER, MALINVERNI, Vol. II).

AVERY Oswald T., MACLEOD Colin M., MCCARTY Maclyn, Studies on the chemical Nature of the substance inducing transformation of pneumococcal types: Induction of transformation by desoxyribonucleic acid fraction isolated from pneumococcus type III, J*ournal of Experimental Medecine* 79 (1944) p. 137-158.

BACHELET Olivier, La hiérarchie des preuves, in Giudicelli-Delage Geneviève (éd.), *Les transformations de l'administration de la preuve pénale: perspectives comparées*, Paris 1997, p. 67-80.

BAERISWYL Bruno, Entwicklungen im Datenschutzrecht/Le point sur le droit de la protection des données, *SJZ* 100 (2004) p. 460-463 (cité: BAERISWYL, Datenschutzrecht).

BAERISWYL Bruno, Videoüberwachung im rechtsfreien Raum? Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten, *DIGMA* 2002 p. 26-28 (cité: BAERISWYL, Videoüberwachung).

MAURER-LAMBROU Urs, VOGT Nedim Peter (éd.), *Datenschutzgesetz*, 3ème éd., Bâle 2014, (cité: BSK-DSG-NOM).

BÄR Walter, Zum Beweiswert der DNA-Analyse, in Donatsch Andreas, Schmid Niklaus (éd.), *Strafrecht und Öffentlichkeit – Festschrift für Jörg Rehberg zum 65. Geburstag*, Zurich 1996, p. 41-51.

BARDIN Laurence, Du téléphone fixe au portable. Un quart de siècle de relations interpersonnelles médiatisées en France, *Cahiers internationaux de sociologie* 2001/1 n° 112 p. 97-122.

BARLIER François, *GALILEO: Un enjeu stratégique, scientifique et technique*, Paris 2008.

BARRELET Denis, Une nouvelle liberté: la liberté des télécommunications, in Cottier Bertil (éd.), *Le droit des télécommunications en mutation*, Fribourg 2001, p. 35-48.

BAUER Alain, FREYNET François, *Vidéosurveillance et vidéoprotection*, Paris 2008.

BAUM Olivier, Rechtliche Fragestellungen im Zusammenhang mit dem kriminalpräventiven Einsatz von Videoüberwachungsanlagen im öffentlichen Raum, *Jusletter* 8 octobre 2007, n° 3.

BAUSCH Stephan, *Videoüberwachung als präventives Mittel der Kriminalitätsbekämpfung in Deutschland und in Frankreich*, Marburg 2004.

BECUE Andy, CHAMPOD Christophe, MARGOT Pierre, *Fingermarks, Bitemarks and other impressions (barefoot, ears, lips) – A review (Septembre 2004 – July 2007)*, Interpol Lyon 2007.

BECUE Andy, CHAMPOD Christophe, EGLI Nicole, MARGOT Pierre, *Fingermarks and Other Impressions Left by the Human Body – A review (August 2007 – July 2010)*, Interpol Lyon 2010.

BECUE Andy, CHAMPOD Christophe, EGLI Nicole, MORET Sébastien, *Fingermarks and Other Impressions – A review (August 2010 – June 2013)*, Interpol Lyon 2010.

BEHNISCH Urs R., Amtshilfe der Schweiz in Steuer(straf)sachen, insbesondere an die USA: Durcheinandertal, *ASA* 77 (2008-2009), p. 737-788.

BELLANGER François, La légalité lorsque l'Etat agit par des moyens de droit privé, in Charles-Albert Morand (éd.), *La légalité: un principe à géométrie variable*, Bâle-Francfort 1991, p. 67-90.

BELSER Eva Maria, EPINEY Astrid, WALDMANN Bernhard (éd.), *Datenschutzrecht – Grundlagen und öffentliches Recht*, Berne 2011, p. 1-51 (cité: DSG-NOM).

BELSER Eva Maria, WALDMANN Bernhard, MOLINARI Eva, *Grundrechte I – Allgemeine Grundrechtslehren*, Zurich – Bâle – Genève 2012.

BÉNÉDICT Jérôme, *Le sort des preuves illégales dans le procès pénal*, Thèse de docotorat, Lausanne 1994.

BENEDICT Nathan, Fingerprints and the Daubert Standard for Admission of Scientifc Evidence: Why Fingerprints Fail and a Proposed Remedy, *Arizona Law Review* 46:519 (2004) p. 519-549.

BENTHAM Jérémie, *Traité des preuves judiciaires*, Vol. I, Paris, 1823 (cité: BENTHAM, Vol. I).

BENTHAM Jérémie, *Traité des preuves judiciaires*, Vol. II, Paris, 1823 (cité: BENTHAM, Vol. II).

BERGIER Sébastien, CARTIER Julien, Les fraudes GSM: détection et contre-mesure – Collaboration entre les organisations et les instances de justice et police – Première partie, *RICPTS* LX (2007) p. 479-492 (cité: BERGIER, CARTIER, RICPTS 2007).

BERGIER Sébastien, CARTIER Julien, Les fraudes GSM: analyse criminelle et poursuite pénale – Collaboration entre les organisations et les instances de justice et police – Seconde partie, *RICPTS* LXI (2008) p. 107-118 (cité: BERGIER, CARTIER, RICPTS 2008).

BERLOVAN Nathalie, L'electronic monitoring en Suisse, *Jusletter* 19 mars 2012, n° 1.

BERNASCONI Paolo, GALLIANI Maria, MARCELLINI Luca, MELI Edy, MINI Mauro, NOSEDA John (éd.), *Codice svizzero di procedura penale (CPP)*, Zurich 2010, p. 501-510 (cité: CPP-Commentario-NOM).

BERTILLON Alphonse, *Identification anthropométrique: instructions signalétiques*, Melun 1893.

BERTOSSA Bernard, Note, *SJ* 1989 p. 397-399.

BETTEX Björn, *L'expertise judiciaire – Etude de droit fédéral et de procédure civile vaudoise*, Thèse de doctorat, Berne 2006.

BIEDERMANN Alex, La valeur probante des indices matériels en sciences forensiques: l'apport de la recherche axée sur les modèles graphiques probabilistes (Réseaux Bayésiens), *RICPTS* LXII (2009) p. 100-103 (cité: BIEDERMANN Alex).

BIEDERMANN August, Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000, *RPS* 120 (2002) p. 77-106 (cité: BIEDERMANN August).

BIRRER Stéphane, TERRETTAZ-ZUFFEREY Anne-Laure, Croisement spatial et temporel des données issues d'activités délictueuses et d'appareils permettant une géolocalisation, *RICPTS* LXI (2008) p. 481-500.

BIRRIEN Jean-Yvon, *Histoire de l'informatique*, 2ème éd., Paris 1992.

BLUMSTEIN Alfred, Science and Technology in Support of Criminal Justice, in LeBlanc Marc, Tremblay Pierre, Blumstein Alfred (éd.), *Nouvelles technologies et justice pénale: XXXVIIIe Cours international de criminologie*, Montréal 1988, Cahier n° 9, p. 2-14.

BOCHET Flore, Utilisation du système AFIS en mode automatique et ses limites dans le processus de décision d'identification en matière d'empreintes digitales, *RICPTS* LXII (2009) p. 106-108.

BOBAY Cédric, RUDER Thomas, Anwendung der Computertomographie bei der odontologischen Leichenidentifikation aus medinzinischer und juristischer Sicht, *forumpoenale* 2015/1 p. 27-32.

BONDALLAZ Stéphane, Le "droit à une télécommunication protégée" ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques, *Jusletter* 25 février 2008, n° 1 (cité: BONDALLAZ, Jusletter).

BONDALLAZ Stéphane, *La protection des personnes et de leurs données dans les télécommunications*, Zurich 2007 (cité: BONDALLAZ, protection des personnes).

BOUGON Yves, TEMMAN Michel, Voyeurisme made in Japan, *Le courrier de l'Unesco* 2001 p. 22-23.

BOULOC Bernard, *Procédure pénale*, 25ème éd., Paris 2016.

BOURCIER Danièle, DE BONIS Monique, *Les paradoxes de l'expertise: savoir ou juger?*, Paris 1999.

BOURGEAULT Guy, L'identification génétique: Enjeux éthiques et politiques, in Hennau-Hublet Christiane, Knoppers Bartha Maria (éd.), *L'analyse génétique à des fins de preuve et les droits de l'homme*, Bruxelles 1997, p. 101-122.

BOVET Christian, Cadre réglementaire des réseaux de téléphonie mobile et politique de la concurrence, *DEP* 2004, p. 689-707.

BRODEUR Jean-Paul, Droit, procédure pénale et technologie, in LeBlanc Marc, Tremblay Pierre, Blumstein Alfred (éd.), *Nouvelles technologies et justice pénale: XXXVIIIe Cours international de criminologie*, Montréal 1988, Cahier n° 9, p. 555-578.

BÜHLER Alfred, Erwartungen des Richters an den Sachverständigen, in *AJP/PJA* 1999 p. 567-574.

BÜLLESFELD Dirk, *Polizeiliche Videoüberwachung öffentlicher Strassen und Plätze zur Kriminalitätsvorsorge*, Hambourg 2002.

BUQUET Alain, *Manuel de criminalistique moderne et de police scientifique*, 5ème éd., Paris 2011.

BUQUET Alain, PASCAL Olivier, Identification d'un individu par la colle des timbres ou des enveloppes, *Revue internationale de police criminelle* 444(1993) p. 27-33.

BURR Kai, *Das DNA-Profil im Strafverfahren unter Berücksichtigung der Rechtsentwicklung in den USA*, Bonn 1995.

BUSCH Heiner, DNA-Analytik vom Ermittlungsautomatismus zum massenhaften Verdacht, *AJP/PJA* 2002 p. 637-643.

CAMPBELL Anthony (Sir), *The Fingerprint Inquiry Report*, Edinbourg 2011.

CAPRIOLI Eric, *Introduction au droit de la sécurité des systèmes d'information*, disponible sur: http://www.caprioli-avocats.net [consulté le 08.05.2016].

CAPT Sébastien, Comprendre, *RICPTS* LXII (2009) p. 80-99.

CARBASSE Jean-Marie, *Histoire du droit pénal et de la justice criminelle*, 2ème éd., Paris 2009 (cité: CARBASSE, Histoire du droit pénal et de la justice criminelle).

CARBASSE Jean-Marie, *Introduction historique au droit pénal*, Paris 1990 (cité: CARBASSE, Introduction historique au droit pénal).

CARNIEL Virginie, Protection de la sphère privée et vidéo surveillance, *sécurIT* du 28 août 2006 p. 17-19.

CARTIER Julien, La recherche et la gestion des liens dans l'investigation criminelle: le cas de la criminalité organisée, *RICPTS* LXII (2009) p. 70-73 (cité: CARTIER, RICPTS).

CARTIER Julien, Localisation des téléphones portables, in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 195-224.

CENTRE DE SERVICES INFORMATIQUES, *Guidelines for Lawful Interception of Telecommunication Traffic – Technical Requirements for Telecommunication Surveillance (TR TS)*, Berne 23 novembre 2011 (cité: CSI-DFJP, Guidelines).

CENTRE NATIONAL DE L'INFORMATION GÉOGRAPHIQUE (CNIG), RFID et localisation, in *fiche du CNIG* n° 111/2007, disponible sur: http://www.cnig.gouv.fr [consulté le 08.05.2016].

CERUZZI Paul E., *A history of modern computing*, 2ème éd., Cambridge – Massachusetts 2003.

CEYHAN Ayse, Enjeux d'identification et de surveillance à l'heure de la biométrie, *Identifier et surveillance – Les technologies de sécurité*, Paris 2006, p. 33-47.

CHAMPOD Christophe, Fingerprint examination: towards more transparency, *Law, Probability and Risk Advance Acess* (2008), vol. 7, p. 111-118 (cité: CHAMPOD, Fingerprint).

CHAMPOD Christophe, Friction Ridge Skin Impression Evidence – Standards of Proof in *Encyclopedia of Forensic Sciences* (2013), vol. 4, p. 111-116 (cité: CHAMPOD, Friction Ridge Skin).

CHAMPOD Christophe, Overview and Meaning of Identification/Individualization in *Encyclopedia of Forensic Sciences* (2013), vol. 3, p. 303-309 (cité: CHAMPOD, Overview).

CHAMPOD Christophe, *Reconnaissance automatique et analyse statistique des minuties sur les empreintes digitales*, Thèse de doctorat, Lausanne 1996 (cité: CHAMPOD, Reconnaissance).

CHAMPOD Christophe, LENNARD Chris, MARGOT Pierre, STOILOVIC Milutin, *Fingerprints and other ridge skin impressions*, Boca Raton – Londre – New York – Washington D.C. 2004.

CHAMPOD Christophe, TARONI Franco, Les préjugés de l'Accusation ou de la Défense dans l'évaluation de la preuve technique, *RPS* 111 (1993) p. 223-235 (cité: CHAMPOD, TARONI, RPS 1993).

CHAMPOD Christophe, TARONI Franco, Probabiliés au procès pénal – risques et solutions, *RPS* 112 (1994) p. 194-219 (cité: CHAMPOD, TARONI, RPS 1994).

CHAMPOD Christophe, VUILLE Joëlle, *Preuve scientifique en Europe: Admissibilité, appréciation et égalité des armes – Etude comparative sur la preuve scientifique établie pour le Bureau du Comité européen pour les problèmes criminels (CDPC du Conseil de l'Europe)*, Lausanne 2010, disponible sur: http://www.coe.int/ [consulté le 08.05.2016].

CHARPIN François, Etymologie et histoire du mot technologie, in *Solaris* n° 4 (1997), disponible sur: http://biblio-fr.info.unicaen.fr/ [consulté le 08.05.2016] (cité: CHARPIN, Solaris n° 4).

CHARVET Sandra, Les conditions de mise en œuvre d'un prélèvement d'ADN lors d'enquêtes de grande envergure et recours contre cette décision (art. 256 CPP), *Jusletter* 21 septembre 2015.

CHASSAING Jean-François, Jurisprudence et sorciers, *Les Cahiers du Centre de Recherches Historiques* 1997 n° 18-19, disponible sur: http://ccrh.revues.org/ [consulté le 08.05.2016].

COHEN Daniel, VERDIER Thierry, BENGHOZI Pierre-Jean, *La mondialisation immatérielle*, Paris 2008.

COMER Douglas E., *TCP/IP: architecture, protocoles et applications*, 5ème éd., Paris 2006.

CONTAT Laurent, MÜLLER Jérémie, Investigation secrète: de la LFIS au Code de procédure pénale suisse; bref état des lieux, *RPS* 130 (2012) p. 311-333.

COQUOZ Raphaël, Profils ADN: matière d'expertise ou élément d'enquête préliminaire?, *RPS* 118 (2000) p. 161-177.

COQUOZ Raphaël, COMTE Jennifer, HALL Diana, HICKS Tacha, TARONI Franco, *Preuve par l'ADN: la génétique au service de la justice*, 3ème éd., Lausanne 2013.

CORBOZ Bernard, In dubio pro reo, *RPS* 111 (1993) p. 403-427.

CORNU Pierre, Les nouvelles technologies au service des autorités de poursuite pénale, in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 237-263.

CRICK Francis, WATSON James Dewey, Molecular structure of nucleic acids: A structure for Deoxyribose Nucleic Acid, *Nature* 171 (1953) p. 737-738.

CURCHOD Jérôme, Les images, la perception visuelle et la communication par l'image en sciences forensiques, *RICPTS* LXII (2009) p. 43-44.

CUSSON Maurice, La surveillance et la télésurveillance: sont-elles efficaces, in *RICPTS* LVIII (2005) p. 131-150 (cité: CUSSON, RICPTS).

CUSSON Maurice, Les nouvelles technologies font-elles baisser la criminalité, in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 65-83 (cité: CUSSON, Nouvelles technologies).

DAS Sajal K., KANT Krishna, ZHANG Nan, *Handbook on Securing Cyber-Physical Critical Infrastructure*, Waltham 2012.

DELOBEL Claude, Les bases de données et le Web, problématique nouvelle ou vieux problèmes?, in Pellegrini Christian, Jacquesson Alain (éd.), *Enseigner l'informatique*, Chêne-Bourg 2001, p. 83-90.

DESBROSSE Xavier, Les empreintes digitales, in *Revue francophone des laboratoires* 392 (2007) p. 51-58.

DILELLIO James, GALVIN Denis, RIZZO Michael, The use of Global Navigation Systems in the Aviation Industry, in Rycroft Michael J. (éd.), *Satellite Navigation Systems: Policy, commercial and technical interaction*, Cambridge – Dordrecht 2003, p. 187-194.

DOCTER Quentin, DUNALEY Emmett, SKANDIER Toby, *CompTIA A+ Complete Deluxe Study Guide: Exams 220-701 (Essentials) and 220-702*, Indianapolis 2009.

DODEL Hans, HÄUPLER Dieter, *Satellitennavigation*, 2ème éd., Berlin 2010.

DONATSCH Andreas, Der Sachverständige im Strafverfahrensrecht, unter besonderer Berücksichtigung seiner Unabhängigkeit sowie des Privatgutachters, *Jusletter* 14 mai 2007, n° 9 (cité: DONATSCH, Jusletter).

DONATSCH Andreas, "DNA-Fingerprinting" zwecks Täteridentifizierung im Strafverfahren, *RPS* 109 (1991) p. 175-196 (cité: DONATSCH, RPS 1991).

DONATSCH Andreas, *Strafrecht III – Delikt gegen Einzelnen*, 10ème éd., Zurich – Bâle – Genève 2013 (cité: DONATSCH, Strafrecht).

DONATSCH Andreas, Überblick über die wesentlichen rechtlichen Grundlagen für das Gutachten Sachverständiger, *Kriminalistik* 61 (2007) p. 566-569 (cité: DONATSCH, Kriminalistik 2007).

DONATSCH Andreas, CAVEGN Claudine, Ausgewählte Fragen zum Beweisrecht nach der schweizerischen Strafprozessordnung, *RPS* 126 (2008) p. 158-173 (cité: DONATSCH, CAVEGN, RPS 2008).

DONATSCH Andreas, CAVEGN Claudine, Entwicklungen im Strafprozessrecht/Le point sur le droit de la procédure pénale, *SJZ* 103 (2007) p. 410-414 (cité: DONATSCH, CAVEGN, SJZ 2007).

DONATSCH Andreas, HANSJAKOB Thomas, LIEBER Viktor (éd.), *Kommentar zur Schweizerischen Strafprozessordnung (StPO)*, 2ème éd., Zurich 2014 (cité: StPO-NOM).

DONATSCH Andreas, SCHWARZENEGGER Christian, WOHLERS Wolfgang, *Strafprozessrecht*, 2ème éd., Zurich 2014.

DONOVAN Thomas J., Techniques de révélation des empreintes digitales latentes, *Revue internationale de police criminelle* 330 (1979) p. 204-206.

DOUTREMEPUICH Christian, Données récentes sur les empreintes génétiques en pratique judiciaire, *Comptes rendus des séances de la Société de biologie et de ses filiales* 192 (1998) p. 963-977.

DOUTREMEPUICH Christian, DOUTREMEPUICH Françoise, Les empreintes génétiques, in Doutremepuich Christian (éd.), *Les empreintes génétiques en pratique judiciaire*, Paris 1998, p. 11-29.

DUCOR Philippe, Protection des bases de données et concurrence déloyale, *Internet* 2003 p. 155-184.

DUHEN Willy, Aspects juridiques des nouveaux services de géolocalisation, in Agostinelli Serge, Augey Dominique, Laurie Frédéric (éd.), *Entre communautés et mobilité*, Tome I, Aix-Marseille 2010, p. 137-152.

DURUPT Béatrice, *La police judiciaire: la scène de crime*, Paris 2000.

EGLI Nicole, Utilisation des scores issus d'un système automatiés d'identification par empreintes digitales pour l'évaluation d'un résultat d'une comparaison entre une trace et une empreinte digitale, *RICPTS* LXII (2009) p. 55-57.

EICKER Andreas, HUBER Roland, *Grundriss des Strafprozessrechts – Mit besonderer Berücksichtigung des Kantons Luzern*, Berne 2014.

EL-RABBANY Ahmed, *Introduction to GPS: the Global Positioning System*, 2ème éd., Norwood 2006.

ELOY Marc, Systèmes informatiques et risques, in Antoine Mireille (éd.), *Le droit de la preuve face aux nouvelle technologies de l'information: aspects techniques et juridiques du transfert et de la conservation des documents*, Namur 1992, p. 4-37.

EMMERSON Ben, ASHWORTH Andrew, MACDONALD Alison, *Human Rights and Criminal Justice*, 3ème éd., Londre 2012.

EPINEY Astrid, HOFSTÖTTER Bernhard, MEIER Annekathrin, THEUERKAUF Sarah, *Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen*, Zurich 2007.

ESCONDIDA Elie, TIMÉLOS Dante, L'apparence de la certitude. L'ADN comme "preuve" scientifique et judiciaire, *actujuridique.com* juillet 2009, disponible sur : http://www.actujuridique.com [consulté le 08.05.2016].

ETIZONI Amitaï, Big Brother ou Big Benefits? Identification biométrique et encartement, in Wuilleumier Anne, Etizoni Amitaï (éd.), *Police et identification: Enjeux, pratiques, techniques*, Paris 2005, p. 9-59.

ETRILLARD Claire, L'enregistrement audiovisuel des auditions de mineurs en France, *RICPTS* LVII (2004) p. 43-54.

EXPERT WORKING GROUP, *Latent print Examination and Human Factors: Improving the Practice throught a Systems Approach*, Washington 2012 (cité: .

EVETT Iw, Expert evidence and forensic misconceptions of the nature of exact science, *Science & Justice* 36 (1996) p. 118-122.

FAULDS Henry, On the Skin-furrows of the Hand, *Nature* 22 (1980) p. 605 (cité: FAULDS, On the Skin-furrows of the Hand).

FERREIRA BROQUET Ludivine, *Le bracelet électronique en Suisse: hier, aujourd'hui et demain*, Thèse de doctorat, Neuchâtel 2015.

FERRO David L., SWEDIN Eric G., *Computers: The life story of a technology*, Westport 2005.

FIAUX Michael, Traquer les délinquants par l'ADN, *Uniscope* 2000-2001 n° 409 p. 3.

FICHET-BOYLE Isabelle, La vidéosurveillance – L'adaptation du système probatoire aux nouvelles technologies, in De Frouville Olivier (éd.), *La preuve pénale: Internationalisation et nouvelles technologies*, Paris 2007, p. 205-230.

FICKENZELLER Klaus, *RFID-Handbuch*, 6ème éd., Munich 2012.

FISCHER Marc Pascal, KUHN André, Elektronischer Zirkulationsbeschluss und dessen Einreichung beim Handelsregisteramt, *REPRAX* 1/2010, p. 1-14.

FLÜCKIGER Alexandre, Droit fondamentaux et vidéosurveillance par les particuliers et les autorités des espaces ouverts au public, in Schwarzenegger Christian, Nägeli Rolf (éd.), *Videoüberwachung als Prävention*, Zurich 2010, p.195-226.

FOX Dirk, Der IMSI-Catcher, in *Datenschutz und Datensicherheit* 26 (2002) p. 212-215.

FRANCHIMONT Michel, JACOBS Ann, MASSET Adrien, *Manuel de procédure pénale*, 4ème éd., Liège 2012.

FRANCILLON Jacques, Génétique et preuve en matière pénale, in Heymann-Doat Arlette (éd.), *Génétique et droits de l'homme*, Paris 1998, p. 143-148.

FURNER Mark, First Forensic Forum Schweiz (F3-CH) Computerforensik und Computerkriminalität, *Recht* 2004 p. 210-212.

GALLUSSER Alain, *L'indice matériel comme moyen de preuve : sa valeur et son utilisation par les magistrats*, Thèse de doctorat, Pully 1998.

GALTON Francis, *Fingerprint*, Londres 1895.

GARRAUD René, *Traité théorique et pratique d'instruction criminelle et de procédure pénale*, Tome I, Paris 1907 (cité: GARRAUD, T. I).

GARRAUD René, *Traité théorique et pratique d'instruction criminelle et de procédure pénale*, Tome II, Paris 1907 (cité: GARRAUD, T. II).

GARSTKA Hansjürgen, Der "nackte" Automobilist im Visier? Datenschutzrechtliche Herausforderungen von "Pay as you drive"-Modellen, *DIGMA* 2007 p. 90-93.

GASCOYNE-BOWMAN Shawn, *Criminal Crafts: From D.I.Y. to F.B.I. Outlaw Projects for Scoundrels, cheats, and armchair detectives*, Missouri 2012.

GAST Matthew, *802.11 Wireless Networks: The Definitive Guide: The Definitive Guide*, 2ème éd., Sebastropol 2005.

GAUTHIER Jean, Enregistrement clandestin d'une conversation téléphonique et preuve pénale, in Hauser Robert, Rehberg Jörg, Stratenwerth Günter (éd.),

Gedächtnisschrift für Peter Noll, Zurich 1984, p. 333-340 (cité: GAUTHIER, Enregistrement clandestin).

GAUTHIER Jean, Les résultats de l'audio-surveillance comme preuve pénale en droit suisse, in *Rapports suisses présentés aux XIIème Congrès international de droit comparé*, Syndey – Melbourne 1986, p. 75-91 (cité: GAUTHIER, Audio-surveillance).

GAUTSCHI Georg, *Der einfache Auftrag: Art. 394-406 OR*, Berne 1971.

GEHRIG Christian, LAHARPE Romano, L'identification médico-légale par l'ADN, in *Médecin et Hygiène* 59 (2001) p. 1801-1807.

GEORGEL Jacques, *Les libertés de communication*, Paris 1996.

GHERNAOUTI-HÉLIE Solange, *La Cybercriminalité : le visible et l'invisible*, Lausanne 2009.

GHERNAOUTI-HÉLIE Solange, DUFOUR Arnaud, *De l'ordinateur à la société de l'information*, Paris 1999.

GIANNALOPOULOS Dimitri, PARIZOT Raphaëlle, La preuve technologique des interceptions et surveillances, in Giudicelli-Delage Geneviève (éd.), *Les transformations de l'administration de la preuve pénale: perspectives comparées*, Paris 1997, p. 245-289.

GILLARDIN Jean, JADOUL Pierre, *L'expertise*, Bruxelles 1994.

GILLÉRON Charles, *L'évolution de la preuve pénale*, Berne 1946.

GIROD Alexandre, MARGOT Pierre, RIBAUX Olivier, WALSH Simon, Base de données ADN: un potentiel peu exploité de mises en relations d'événements criminels, *RICPTS* LVII (2004) p. 131-147.

GISLER Frédéric, *La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée*, Zurich 2009.

GLESS Sabine, Strafverfolgung im Internet, *RPS* 130 (2012) p. 3-22.

GODENZI Gunhild, *Private Beweisbeschaffung in Strafprozess*, Zurich 2008.

GOLDSCHMID Peter, *Der Einsatz technischer Überwachungsgeräte im Strafprozess: unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern*, Berne 2001 (cité: GOLDSCHMID, Überwachung).

GOLDSCHMID Peter, Geheime Überwachungsmassnahmen im Entwurf zu einer eidgenössischen Strafprozessordnung, in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 157-172 (cité: GOLDSCHMID, Überwachungsmassnahmen).

GOLDSCHMID Peter, MAURER Thomas, SOLLBERGER Jürg (éd.), *Kommentierte Textausgabe zur Schweizerischen Starfprozessordnung (StPO) vom 5. Oktober 2007*, Berne 2008, (cité : GOLDSCHMID, MAURER, SOLLBERGER, Textausgabe-NOM).

GRABENWARTER Christoph, PABEL Katharina, *Europäische Menschenrechtskonvention – Eine Studienbuch*, 5ème éd., Munich – Bâle – Vienne 2012.

GRIESE Joachim, SIEBER Pascal, Internet als erste Ausbaustufe des Information Highway, in Hilty Reno (éd.), *Information Highway - Beiträge zu rechtlichen und tatsächlichen Fragen*, Berne 1996, p. 43-63.

GRIMM Thomas, "Pay as you drive" – Die Technik Vergleich der Techniken zur Sammlung von Nutzungsdaten im Fahrzeug-Umfeld, *DIGMA* 2007 p. 94-97.

GRISEL André, La liberté personnelle et les limites du pouvoir judiciaire, *Revue internationale de droit comparé* 1975 n° 3 p. 550-570 (cité: GRISEL A.).

GRISEL Etienne, *Droits fondamentaux – Libertés idéales*, Berne 2008 (cité: GRISEL E.).

GUINCHARD Serge, BUISSON Jacques, *Procédure pénale*, 10ème éd., Paris 2014.

GUNN Alan, *Essential forensic biology*, 2ème éd., Chichester 2009.

GYSIN Roland, Der Fingerabdruck steht unter Verdacht, *Plädoyer* 6/2005 p. 11-13.

HAEFGLIGER Athur, SCHÜRMANN Frank, *Die Europäische Menschenrechtskonvention und die Schweiz : die Bedeutung der Konvention für die schweizerische Rechtspraxis*, 2ème éd., Berne 1999.

HÄFELIN Ulrich, HALLER Walter, KELLER Helen, *Schweizerisches Bundesstaatsrecht*, 8ème éd., Zurich 2012.

HALLER Walter, *The Swiss Constitution in a comparative context*, Zurich 2009.

HÄNER Isabelle, Mindestgarantien für Strafverfahren und ihre Bedeutung für verwaltungsrechtliche Sanktionen, in Häner Isabelle, Waldmann Bernhard (éd.), *Verwaltungsstrafrecht und sanktionerendes Verwaltungsrecht*, Zurich 2010, p. 19-40.

HANSJAKOB Thomas, Nr. 45 Bundesgericht, Strafrechtliche Abteilung, Urteil vom 9. Oktober 2007 i.S. X. gegen Oberstaatsanwaltschaft des Kantons Zürich (Beschwerde in Strafsachen) – 6B_170/2007, BGE 133 IV 329, *forumpoenale* 2008/4 p. 212-215 (cité: HANSJAKOB, forumpoenale).

HANSJAKOB Thomas, *BÜPF/VÜPF – Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*, 2ème éd., St-Gall 2006 (cité: HANSJAKOB, BÜPF/VÜPF).

HANSJAKOB Thomas, Das neue Bundesgesetz über die verdeckte Ermittlung, *RPS* 122 (2004) p. 97-114 (cité: HANSJAKOB, verdeckte Ermittlung).

HANSJAKOB Thomas, Der Einsatz von GovWare in der Schweiz – Zum geplanten Art. 269ter StPO, *Jusletter-IT* 15 mai 2014 (cité: HANSJAKOB, art. 269ter StPO).

HANSJAKOB Thomas, Einführung von GovWare weiterhin auf Kurs – Zum Revision von Art. 269ter im Rahmen der laufenden BÜPF-Revision, *Jusletter-IT* 24 septembre 2015 (cité: HANSJAKOB, Jusletter-IT).

HANSJAKOB Thomas, Einsatz von GovWare – zulässig oder nicht?, *Jusletter* 5 décembre 2011, n° 1 (cité: HANSJAKOB, GovWare).

HANSJAKOB Thomas, Geheime Erhebung von Beweisen nach StPO, *forumpoenale* 2011/5 p. 299-309 (cité: HANSJAKOB, forumpoenale 2011).

HANSJAKOB Thomas, Grenzen und Rahmenbedingungen der verdeckten präventiven Tätigkeit der Polizei, *forumpoenale* 2015/1 p. 33-36 (cité: HANSJAKOB, forumpoenale 2015).

HANSJAKOB Thomas, Zur Zulässigkeit von Antennensuchläufen – Bemerkungen zu BGE 1B_376/2011, *Jusletter* 5 mars 2012, n° 1 (cité: HANSJAKOB, Antennensuchläufen).

HANSJAKOB Thomas, Zwangsmassnahmen in der neuen Eidg. StPO, *RPS* 126 (2008) p. 90-114 (cité: HANSJAKOB, Zwangsmassnahmen).

HÄRING Daniel, Verwertbarkeit rechtswidrig erlangter Beweise gemäss Schweizerischer Strafprozessordnung - alte Zöpfe oder substanzielle Neuerungen?, *RPS* 127 (2009) p. 225-257.

HARRIS David, O'BOYLE Michael, WARBRICK Colin, *Law of the European Convention on Human Rights*, 3ème éd., Oxford – New York 2014.

HAURI Max, Zurich, Bezirksgericht 1. Abt. 7.12.1993, *SJZ* 90 (1994) p. 402-405.

HAUSER Robert, SCHWERI Erhard, HARTMANN Karl, *Schweizerisches Strafprozessrecht*, 6ème éd., Bâle 2005.

HAUSHEER Heinz, Die Genanalyse zu Identifizierungszwecken im Straf-, Zivil- und Veraltungsrecht, *RPS* 117 (1998) I p. 449-472.

HEER Marianne, 4. Titel: Beweismittel – 5. Kapitel: Sachverständige, in Niggli Marcel Alexander, Heer Marianne, Wiprächtiger Hans (éd.), *Schweizerische Strafprozessordnung – Jugendstrafprozessordnung*, 2ème éd., Bâle 2013, p. 1391-1476.

HEILMANN Andreas, En quête d'identité: Les empreintes génétiques et l'identification judiciaire, in Heilmann Eric (éd.), *Science ou justice? Les savants, l'ordre et la loi*, Paris 1994, p. 30-41.

HEINIGER André, Schrankenlose Fernmeldeüberwachung aufgrund eines konzeptionellen Fehlers im BÜPF?, *Jusletter* 17 septembre 2012, n° 2.

HENRY Edward Richard, *Classification and Uses of Finger Prints*, Londres 1900.

HERSCHEL William, Skin Furrows of the Hand, *Nature* 23 (1880) p. 76.

HESLER Nicole Duval, L'admissibilité des nouvelles théories scientifiques, *Revue du Barreau* 62 (2002) p. 359-385.

HIBBERT Michelle, DNA Databanks: Law enforcement's greatest surveillance tool?, *Wake Forest Law Review* vol. 34 (1999) p. 767-825.

HODGES Steve, MCFARLANE Ducan, RFID: le concept et incidence, in OCDE (éd.), *L'économie de la sécurité*, Paris 2004, p. 61-85.

HOLDER Eric H. Jr, ROBINSON Laurie O., LAUB John H., *The Fingerprint Soucrebook*, Washington 2011 (cité: HOLDER, ROBINSON, LAUB-NOM).

HOTTELIER Michel, La réglementation du domaine public à Genève, *SJ* 2002 p. 123-175 (cité: HOTTELIER, SJ 2002).

HOTTELIER Michel, Les garanties de procédure, in Thürer Daniel, Aubert Jean-François, Müller Jörg Paul (éd.), *Verfassungsrecht der Schweiz – Droit constitutionnel suisse*, Zurich 2001, p. 809-822 (cité: HOTTELIER, Garanties de procédure).

HOTTELIER Michel, MOCK Hanspeter, PUÉCHAVY Michel, *La Suisse devant la Cour européenne des droits de l'homme*, 2ème éd., Zurich 2011.

HÜGLI Heinz, PIGUET Christian, *Du zéro à l'ordinateur*, Lausanne 2004.

HURTADO POZO José, *Droit pénal – Partie spéciale*, Nouvelle éd. Refondue et augmentée, Genève – Zurich – Bâle 2009.

HUYGHE François-Bernard, *ADN et enquêtes criminelles*, Paris 2008 (cité: HUYGHE, ADN).

HUYGHE François-Bernard, *Ecoutes téléphoniques, traces et interceptions : La vie numérique des autres*, Paris 2008, disponible sur : http://www.huyghe.fr [consulté le 08.05.2016] (cité: HUYGHE, La vie numérique).

HUYGHE François-Bernard, *Les écoutes téléphoniques*, Paris 2009 (cité: HUYGHE, Ecoutes téléphoniques).

ILL Christoph, Konfrontationsanspruch: Einschränkung und Kompensation, *forumpoenale* 2010/3 p. 162-168.

INTERNATIONAL TELECOMMUNICATION UNION, *50 years of excellence: 1956-2006*, Genève 2006 (cité: UIT).

JACCARD Michel, Forme, preuve et signature électronique, in Jeanneret Vincent (éd.), *Aspects juridiques du commerce électronique*, Zurich 2001, p. 113-155.

JACKSON Graham, The scientist and the Scales of Justice, *Science & Justice* 40 (2000) p. 81-85.

JACOB Benjamin, JACOB Julie, *Les SMS: les nouvelles formes de preuve*, Paris 2007, disponible sur : http://www.pdgb.com [consulté le 08.05.2016].

JAGGI Emanuel, Die Revision des BÜPF, *RPS* 133 (2015) p. 276-294.

JEAN-RICHARD-DIT-BRESSEL Marc, Die Mailbox – Ziel oder Weg?, *RPS* 125 (2007) p. 157-179 (cité: JEAN-RICHARD-DIT-BRESSEL, Mailbox).

JEAN-RICHARD-DIT-BRESSEL Marc, Ist ein Millionendiebstahl ein Bagatelldelikt? – Fragen zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000, *RPS* 119 (2001) p. 40-70 (cité: JEAN-RICHARD-DIT-BRESSEL, BÜPF).

JEANNERET Yvan, KÜHN André, *Précis de procédure pénale*, Berne 2013.

JEFFREYS Alex, Hypervariable "minisatellites" regions in human, in *Nature* 314 (1985) p. 67-73.

JERLOV Emile, Projet de système de classification plantaire chez les nouveaux-nés, *Acta obstetricia et gynecologica scandinavia*, vol. 9 (1930) p. 267-281.

JOBARD Fabien, SCHULZE-ICKING Niklas, *Preuves hybrides: L'administration de la preuve pénale sous l'influence des techniques et des technologies*, Guyancourt 2004, n° 96.

JORNS Olivier, ZHENDONG Ma, Wo bin ich, wo sind wir, wo ist alles? - Ortsbezogene Dienste bieten Vorteile und immense Möglichkeiten, allerdings auch Gefahr des Verlusts der Privatsphäre, *DIGMA* 2011 p. 30-36.

JOSEPH Sarah, SCHULTZ Jenny, CASTAN Melissa, *The international covenant on civil and political rights: cases, materials and commentary*, 2ème éd., Oxford 2004.

JOSITSCH Daniel, *Grundriss des schweizerischen Strafprozessrechts*, 2ème éd., Zurich – Saint-Gall 2013 (cité: JOSITSCH, Strafprozessrechts).

JOSITSCH Daniel, Wenn polizeiliche Ermittler im Chatroom in Teufels Küche kommen - oder wie das Bundesgericht neue Probleme geschaffen hat, *AJP/PJA* 2011 p. 181-191 (cité: JOSITSCH, Chatroom).

JOSITSCH Daniel, MULLE Franziska, Die StPO-Revision in Bezug auf die Bestimmungen über die verdeckte Ermittlung, *AJP/PJA* 2014 p. 491-498.

JOTTERAND Olivier, MÜLLER Jérémie, TRECCANI Jean, L'utilisation du cheval de Troie comme mesure de surveillance secrète, *Jusletter* 21 mai 2012, n° 4.

KÄLIN Walter, EPINEY Astrid, CARONI Martina, KÜNZLI Jörg, *Völkerrecht – Eine Einführung*, 3ème éd., Berne 2010.

KATZENSTEIN Annegret, EUGSTER Luziuzs, 5. Titel: Zwangsmassnahmen – 8. Kapitel: Geheime Überwachungsmassnahmen in Niggli Marcel Alexander, Heer Marianne, Wiprächtiger Hans (éd.), *Schweizerische Strafprozessordnung – Jugendstrafprozessordnung*, Bâle 2011, p. 2198-2221.

KAUFMANN Martin, *Beweisführung und Beweiswürdigung – Tatsachenfeststellung im schweizerischen Zivil-, Straf- und Verwaltungsprozess*, Zurich 2009.

KAYE D.H, The relevance of "Matching" DNA: Is the window half open or half shut?, *The Journal of Criminal Law & Criminology* 85 (1995) n° 3 p. 676-695.

KILLIAS Martin, HAAS Henriette, TARONI Franco, MARGOT Pierre, Quelles catégories de condamnés devrait-on faire figurer dans une banque de profils ADN, in Cassani Ursula, Dittman Volker, Maag Renie, Steiner Silvia (éd.), *Mehr Sicherheit – weniger Freiheit? – Plus de sécurité – moins de liberté?*, Zurich 2003, volume 21, p. 295-309.

KLAUSER Francisco, A Comparision of the Impact of Protective and Preservative Video Surveillance on Urban Territoriality: the Case of Switzerland, *Surveillance & Society* 2004 2(2/3) p. 145-160 (cité: KLAUSER, CCTV).

KLAUSER Francisco, Die Veränderung der urbanen Territorialität infolge der Videoüberwachung des öffentlichen Raumes: ein Vergleich unterschiedlicher räumlicher Funktionsweisen der Videoüberwachung, *Geographica Helvetica* 2004 (59/2) p. 106-118 (cité: KLAUSER, Videoüberwachung).

KLAUSER Francisco, *Die Videoüberwachung als Aneignungsform öffentlicher Räume*, Thèse de doctorat, Frankfurt am Main 2006 (cité: KLAUSER, Thèse).

KLEY Andreas, Der Grundrechtskatalog der nachgeführten Bundesverfassung – ausgewählte Neureungen, *ZBJV* 1999/6 p. 301-347.

KLUMPE Birgit, *Der "genetische Fingerabdruck" im Strafverfahren – Rechtsprobleme bei der Anwendung genetischer Analysen im Grossbritannien und Deutschland*, Freiburg im Breisgau 1993.

KNAPP Blaise, *Précis de droit administratif*, 4ème éd., Bâle – Francfort-sur-le-Main 1991.

KNODEL Tanja, 5. Titel: Zwangsmassnahmen – 8. Kapitel: Überwachungsmassnahmen, in Niggli Marcel Alexander, Heer Marianne, Wiprächtiger Hans (éd.), *Schweizerische Strafprozessordnung – Jugendstrafprozessordnung*, Bâle 2013, p. 2005-2063.

KNOPPERS Bartha Maria, GRIMAUD Marie Angèle, CHOQUETTE Catherine, LE BRIS Sonia, Les tests génétiques à des fins d'identification, in Colloque international, *Analyse génétique humaine et protection de la personnalité*, Lausanne 1994, p. 57-101.

KNOWLES A.M., Aspects of physicochemical methods fort he detection of latent fingerprints, *Journal of Physics E: Scientific Instrument* 11 (1978) p. 713-721.

KÖLLER Norbert, NISSEN Kai, RIESS Michael, SADORF Erwin, *Probabilistische Schlussfolgerungen in Schriftgutachten – Zur Begründung und Vereinheitlichung von Wahrscheinlichkeitsaussagen im Sachverständigengutachten*, Munich 2004.

KÔZÔ Watanabe, Interroger le Sphinx: Genèse et structure de la modernité identitaire, in Hasumi Shiguehiko, Meschonnic Henri (éd.), *La modernité après le post-moderne*, Paris 2002, p. 61-70.

KUHN André, JEANNERET Yvan (éd.), *Commentaire romand du Code de procédure pénale suisse*, Bâle 2011 (cité : CR-CPP-NOM).

KUHN André, PERRIER Camille, Quelques points problématiques du Code de procédure pénale suisse, *Jusletter* 22 septembre 2008, n° 2.

KÜPPER Axel, *Location-Based Services : Fundamentals and Operation*, Chichester 2005.

LAINGUI André, LEBIGRE Arlette, *Histoire du droit pénal: La procédure criminelle*, Tome II, Paris 1979.

LANZI Lorenzo, CORREVON Daniel, SAPIN Eric, DE PRIESTER Jean-Philippe, Etude de cas: évaluation de la vitesse d'un véhicule enregistré par une caméra de surveillance, *RICPTS* LIX (2006) p. 233-238.

LAPOINTE Manon, L'identification par l'analyse génétique dans le système de preuve pénale canadien: A la recherche du difficile équilibre entre la poursuite de la vérité et les droits fondamentaux de l'accusé, in Hennau-Hublet Christiane, Knoppers Bartha Maria (éd.), *L'analyse génétique à des fins de preuve et les droits de l'homme*, Bruxelles 1997, p. 227-256.

LAPORTE Michel, *Consultation publique – L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics*, Québec 2004.

LATHOUD Bertrand, Technologie de l'information et limites des moyens de preuves, in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 173-193.

LAUDON Kenneth, LAUDON Janet, FIMBEL Eric, COSTA Serge, *Management des systèmes d'information*, 11ème éd., Upper Saddle River 2010.

LAVENUE Jean-Jacques, VILLALBA Bruno, *Vidéo-surveillance et détection automatique des comportements anormaux - Enjeux techniques et politiques*, Lille 2011.

LAVERGNE Léo, Deux aspects de l'identification génétique en médecine légale : la position du généticien dans ce nouvel environnement et l'évaluation de rareté des profils génétique, in Hennau-Hublet Christiane, Knoppers Bartha Maria (éd.), *L'analyse génétique à des fins de preuve et les droits de l'homme*, Bruxelles 1997, p. 39-78.

LE DOUARIN Nicole, *Science et justice: Des empreintes digitales aux empreintes génétiques, à la recherche de la preuve indiscutable*, Paris 2004.

LECLERC Henri, L'intime conviction du juge: Norme démocratique de la preuve, in Centre universitaire de recherches administratives et politiques de Picardie (éd.), *Le for intérieur*, Paris 1995, p. 206-213 (cité: LECLERC H.).

LECLERC Olivier, L'indépendance de l'expert, in Favro K (éd.), *L'expertise: enjeux et pratiques*, Paris 2009, p. 167-180 (cité: LECLERC O.).

LEGLER Thomas, *Vie privée, image volée: la protection de la personnalité contre les prises de vues*, Berne 1997.

LEICK Alfred, *GPS satellite surveying*, 3ème éd., New Jersey 2004.

LEMAN-LANGLOIS Stéphane, BRODEUR Jean-Paul, Les technologies de l'identification – Une note de recherche, *RICPTS* LVIII (2005) p. 69-82.

LEMPERT Richard O., Some caveats concerning DNA as criminal identification evidence: with thanks to the Reverend Bayes, *Cardozo Law reviews* n° 13 p. 303-341.

LÉVY Jacques, Espace public, in Lévy Jacques, Lusseault Michel (éd.), *Dictionnaire de la géographie*, p. 336-339 (cite: LÉVY J.).

LÉVY Vanessa, *Le droit à l'image – Définition, protection, exploitation – Etude de droit privé*, Zürich 2002(cite: LÉVY V.).

LEUPOLD Michael, Die Schweizerische Strafprozessordnung vom 5. Oktober : Entstehung – Grundzüge – Besonderheiten, *BJM* 2008 p. 233-258.

LEZEAU Thierry, Prélèvement sur scène de crime, in Doutremepuich Christian (éd.), *Les empreintes génétiques en pratique judiciaire*, Paris 1998, p. 35-41.

LINDLEY Dennis, That wretched prior, *Significiance Magazine* 2004 p. 85-87.

LOCARD Edmond, *Traité de criminalistique – Les empreintes et les traces dans l'enquête criminelle*, T. I-II, Lyon 1931 (cité: LOCARD, T. I-II).

LOCARD Edmond, *Traité de criminalistique – Les preuve de l'identité*, T. II-III, Lyon 1932 (cité: LOCARD, T. II-III).

MALAUZAT Marie-Isabelle, *Le droit face aux pouvoirs des données génétiques*, Aix-en-Provence 2000.

MANAOUIL Cécile, WERBROUCK Annabelle, TRAULLE Emilie, CORDIER Alice, GIGNON Maxime, JARDE Olivier, Le Fichier national automatisé des empreintes génétiques (FNAEG): fonctionnement, intérêts et limites, in *Médecin & Droit* 88 (2008) p. 17-23.

MANGIN Patrice, TARONI Franco, L'expert et la preuve génétique ADN: le rapport analytique est-il encore suffisant?, *RSJ* 94 (1998) p. 505-511.

MARGOT Pierre A., CHAMPOD Christophe, La preuve dactyloscopique et la preuve par l'ADN: vers une unité de doctrine dans l'évaluation de leur force probante, *RPS – Le droit pénal et ses liens avec les autres branches du droit* 114 fasc. spécial (1996) p. 229-248.

MARGOT Pierre A., LENNARD Chris, Traces et empreintes: Le point sur les nouvelles techniques, *Revue internationale de police criminelle* 441 (1993) p. 10-18 (cité: MARGOT, LENNARD, RIPC).

MARGOT Pierre A., LENNARD Chris, *Les méthodes de détection des empreintes digitales*, 6ème éd., Lausanne 1994 (cité : MARGOT, LENNARD, Empreintes).

MARTIN David, *Les fichiers de police*, Paris 1999 (cité: MARTIN D.).

MARTIN Keith M., *Everyday Cryptography: Fundamental Principles and Applications*, New York 2012 (cité: MARTIN K.)

MARTY Bernard, MONIN Henri, *Le premier âge de l'ADN*, Paris 2003.

MASTRONARDI Philippe, Menschenwürde als materielle "Grundnorm" des Rechtsstates?, in Thürer Daniel, Aubert Jean-François, Müller Jörg Paul (éd.), *Verfassungsrecht der Schweiz – Droit constitutionnel suisse*, Zurich 2001, p. 233-245.

MATELLY Jean-Hugues, Influence de la preuve génétique dans l'enquête judiciaire, in Doutremepuich Christian (éd.), *10 ans d'empreintes génétiques*, Paris 2001, p. 121-136.

MATTERN Friedemann, Die technische Basis für das Internet der Dinge, in Fleisch Elgar, Mattern Friedemann (éd.), *Das Internet der Dinge - Ubiquitious Computing und RFID in der Praxis*, Berlin 2005.

MAURER Thomas, *Das bernische Strafverfahren*, 2ème éd., Berne 2003.

MAURER-LAMBROU Urs, VOGT Nedim Peter (éd.), *Datenschutzgesetz*, 3ème éd., Bâle 2014, (cité: BSK-DSG-NOM).

MCDONALD William H, L'enregistrement des aveux au magnétoscope, in *Revue internationale de police criminelle* 386 (1985) p. 78-80.

MEIER Andreas, *Relationale Datenbanken*, 4ème éd., Fribourg 2002 (cité: MEIER A.).

MEIER Philippe, *Protection des données : fondements, principes généraux et droit privé*, Berne 2011 (cité: MEIER P.).

MENOTTI-RAYMOND Marilyn A., DAVID Victor A., O'BRIEN Stephen J., Pet cat hair implicates murder suspect, *Nature* 386 (1997) p. 774.

MERLE Roger, VITU André, *Traité de droit criminel: Problèmes généraux de la science criminelle – Droit pénal général*, Tome I, 7ème éd., Paris 1997 (cité: MERLE/VITU, T. I).

MERLE Roger, VITU André, *Traité de droit criminel: Procédure pénale*, Tome II, 5ème éd., Paris 2001, (cité: MERLE/VITU, T. II).

MÉTILLE Sylvain, Infrastructures et données informatiques: quelle protection au regard du Code pénal suisse, *RPS* 132 (2014) p. 283-316 (cité: MÉTILLE-RPS).

MÉTILLE Sylvain, L'utilisation privée des moyens techniques de surveillance et la procédure pénale, in Dunand Jean-Philippe, Mahon Pascal (éd.), *"Le droit décloisonné", interférences et interdépendances entre droit privé et droit public*, Zürich 2009, p. 179-198 (cité: MÉTILLE, Surveillance privée).

MÉTILLE Sylvain, Les mesures de surveillance prévues par le CPP, *Jusletter* 19 décembre 2011, n° 2 (cité: MÉTILLE, Jusletter).

MÉTILLE Sylvain, *Mesures de techniques de surveillance et respect des droits fondamentaux – en particulier dans le cadre de l'instruction pénale et du renseignement*, Thèse de doctorat, Bâle 2011 (cité: MÉTILLE, Thèse).

MÉTRAILLER Jean-Pierre, SCHURTZ-Taylor Jane, Liens et nœuds: aspects techniques des nouveaux moyens de télécommunication, in Cottier Bertil (éd.), *Le droit des télécommunications en mutation*, Fribourg 2001, p. 21-32.

MEUNIER Julie, La notion de procès équitable devant la Cour européenne des droits de l'Homme, in Ruiz Fabri Hélène (éd.), *Procès équitable et enchevêtrement des espaces normatifs*, Paris 2003, p. 185-208.

MEUWLY Didier, *Reconnaissance de locuteurs en sciences forensiques: l'apport d'une approche automatique*, Lausanne 2001.

MEYER Frank, Art. 6 Recht auf ein faires Verfahren, in Karpenstein Ulrich, Mayer Franz (éd.), *EMRK – Konvention zum Schutz der Menschenrechte und Grundfreiheiten*, 2ème éd., Munich 2015.

MEYER Ulrike, WETZEL Susanne, A Man-in-the-Middle Attack on UMTS, *Proceedings of the ACM Workshop on Wireless Security (WiSe)* 2004 p. 90-97.

MEYER-LADEWIG Jens, *EMRK – Europäische Menschenrechtskonvention*, 3ème éd., Baden-Baden 2011.

MONNIER Gilles, *Le droit d'accès aux données personnelles traitées par un média : droit suisse de la personnalité – aspects de droit constitutionnel, de droit pénal et de droit de procédure*, Berne 1999 (cité: MONNIER, Droit d'accès).

MONNIER Gilles, Le hacking: enjeux actuels à la lumière du cas "Hacker-Croll", *Medialex* 3/2010 p. 130-133 (cité: MONNIER, Hacking).

MONNIER Gilles, Le piratage informatique en droit pénal, *Sic!* 3/2009 p. 141-153 (cité: MONNIER, Piratage).

MONTAGNÉ Jean-Claude, *Transmissions: l'histoire des moyens de communication à distance: à la découverte de l'évolution des moyens de communication à distance au cours des âges, depuis l'antiquité jusqu'au milieu du XXème siècle: du sifflet préhistorique… à la télévision*, Bagneux 2008.

MOOR Pierre, FLÜCKIGER Alexandre, MARTENET Vincent, *Droit administratif – Les fondements*, vol. 1, 3ème éd., Berne 2012.

MOOR Pierre, POLTIER Etienne, *Droit administratif – Les actes administratifs et leur contrôle*, vol. 2, 3ème éd., Berne 2011.

MOREILLON Laurent, La recherche des preuves dans l'instruction pénale: maxime inquisitoire et droits de la défense, *RPS* 122 (2004) p. 140-158.

MOREILLON Laurent, BLANK Sandra, La surveillance policière et judiciaire des communications par Internet, *Medialex* 2/2004 p. 81-90.

MOREILLON Laurent, PAREIN-REYMOND Aude, *Petit commentaire du CPP – Code de procédure pénale*, Bâle 2013.

MORSINK Johannes, *The Universal Declaration of Human Rights: origins, drafting, and intent*, Philadelphia 1999.

MOUSTIERS Anaïs, Preuve et biotechnologies : l'utilisation des empreintes génétiques à des fins judiciaires – L'adaptation du système probatoire aux nouvelles technologies, in De Frouville Olivier (éd.), *La preuve pénale: Internationalisation et nouvelles technologies*, Paris 2007, p. 165-204.

MUGGLI Sandra, *Im Netz ins Netz – Pädokriminalität im Internet und der Einsatz von vedeckten Emittlern und vedeckten Fahndern zu deren Bekämpfung*, Zurich 2014.

MÜLLER Jérémie, *La cybercriminalité économique au sens étroit - Analyse approfondie du droit suisse et aperçu de quelques droits étrangers*, Lausanne 2012 (cité : MÜLLER Jérémie.

MÜLLER Jörg P., Allgemeine Bemerkungen zu den Grundrechten, in Thürer Daniel, Aubert Jean-François, Müller Jörg Paul (éd.), *Verfassungsrecht der Schweiz – Droit constitutionnel suisse*, Zurich 2001, p. 621-645.

MÜLLER Jörg P., SCHEFER Markus, *Grundrechte in der Schweiz – Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte*, 4ème éd., Berne 2008.

MÜLLER Markus, WYSSMANN Ursula, Polizeiliche Videoüberwachung – Rechtssetzungszuständigkeit nach bernischem Polizeigesetz, *BVR/JAB* 12/2005 p. 529-554.

MULLIS Annina, Grenzen präventiver erkennungsdienstlicer Behandlung und DNA-Probenahme, *forumpoenale* 2015/5 p. 308-313.

MURRAY Andrew, *The Regulation of Cyberspace: Control in the Online Environment*, New York 2007.

NIGGLI Marcel Alexander, HEER Marianne, WIPRÄCHTIGER Hans (éd.), *Schweizerische Strafprozessordnung – Jugendstrafprozessordnung*, 2ème éd., Bâle 2014 (cité: BSK-StPO-NOM).

NOLL Peter, *Strafprozessrecht*, Zurich 1977.

OBERHOLZER Niklaus, DNA Datenbanken Pro und Kontra – ein öffentlicher Disput, in Cassani Ursula, Dittman Volker, Maag Renie, Steiner Silvia (éd.), *Mehr Sicherheit – weniger Freiheit? – Plus de sécurité – moins de liberté?*, Zurich 2003, volume 21, p. 327-334 (cité: OBERHOLZER, DNA).

OBERHOLZER Niklaus, *Grundzüge des Strafprozessrechts: dargestellt am Beispiel des Kantons St.Gallen*, 3ème éd., Berne 2012 (cité: OBERHOLZER, Strafprozessrechts).

OBERSON Xavier, Récents développements dans le droit de l'assistance internationale en matière fiscale, notamment avec les Etats-Unis : sept leçons à tirer de « l'affaire UBS », in Bellanger François, de Werra Jacques (éd.), *Genève au confluent du droit interne et du droit international – Mélanges offerts à la Faculté de droit de l'Université de Genève à la Société Suisse des Juristes à l'occasion du Congrès 2012*, Genève 2012, p. 135-164.

OOSTERLINK René, Localisation par satellite: GALILEO, in Organisation de coopération et de développement économiques (OCDE) (éd.), *L'économie de la sécurité*, Paris 2004, p. 61-85.

O'REGAN Gerard, *A Brief History of Computing*, 2ème éd., Londre 2012.

PADOVA Yann, A la recherche de la preuve absolue – Réflexions sur l'utilisation de l'ADN en procédure pénale et sur le développement des fichiers d'empreintes, *Archives de politique criminelle* 2004/1 n° 26 p. 71 à 90.

PAOLETTI Félix, L'histoire de l'informatique, in Baron Georges-Louis, Paoletti Félix, Raynaud (éd.), *Informatique, communication et société*, Paris 1993, p. 41- 49.

PAREIN Saskia, Les preuves illégales recueillies par les particuliers sous l'empire du Code de procédure pénale suisse, *Jusletter* 8 octobre 2012, n° 2.

PAULING Linus, COREY Robert B., A proposed structure for the nucleic acids, *Proceedings of the national academy of sciences* 39 (1953) p. 84-97.

PAYCHÈRE François, Le juge et l'expert – Plaidoyer pour une meilleure comprehension, in *L'expertise médicale*, vol. 1, Chêne-Bourg – Genève 2002-2008, p. 133-150.

PERES Michael, *The focal encyclopedia of photography*, 4ème éd., Burlington – Oxford 2007.

PERRIER Camille, VUILLE Joëlle, *Procédure pénale suisse – Tables pour les études et la pratique*, 2ème éd., Bâle 2011.

PERRIER DEPEURSINGE Camille, *CPP Annoté – PPMin, LTF, LAVI, DPA, LOAP et droit cantonal romand d'application du CPP*, Bâle 2015.

PETTITI Louis-Edmond, Droit au silence, *Docmentação e Direito Comparado* 1998 n° 75/76 p. 135-148.

PETTITI Louis-Edmon, DÉCAUX Emmanuel, IMBERT Pierre-Henri (éd.), *La convention européenne des droits de l'homme: Commentaire article par article*, 2ème éd., Paris 1999 (cité: CEDH-NOM).

PFEFFERLI Peter W., Daktyloskopie: Neuer Perspektiven bei Spurensicherung und Spurenauswertung, *Kriminalistik* 51 (1997) p. 217-221.

PIETH Mark, *Schweizerisches Strafprozessrecht: Grundriss für Studium und Praxis*, 2ème éd., Bâle 2012.

PIQUEREZ Gérard, La preuve pénale – Présentation générale, *RJJ* 2004 p. 7-23 (cité: PIQUEREZ, RJJ 2004).

PIQUEREZ Gérard, Risque de fuite, droit au silence et présomption d'innocence, *RJJ* 1994 p. 285-291 (cité: PIQUEREZ, RJJ 1994).

PIQUEREZ Gérard, *Traité de procédure pénale suisse*, 2ème éd., Zurich 2006 (cité: PIQUEREZ, Traité de procédure pénale suisse).

PIQUEREZ Gérard, MACALUSO Alain, *Procédure pénale suisse*, 3ème éd., Zurich 2011.

PISANI Camille, *Meurtre au Muséum: Dossier didactique*, Bruxelles 2006.

PITTELOUD Jo, *Code de procédure pénale suisse (CPP) – Commentaire à usage des praticiens*, St-Gall 2012.

RAHOUAL Malek, SIARRY Patrick, *Réseaux informatiques: conception et optimisation*, Paris 2006.

RAINER J. Schweizer, Verfassungsrechtlicher Persönlichkeitsschutz, in Thürer Daniel, Aubert Georg, Müller Jean-François (éd.), *Verfassungrecht der Schweiz = Droit constitutionnel suisse*, Zurich 2001, p. 691-706.

RASSAT Michèle-Laure, *Traité de procédure pénale*, Paris 2001.

RÉMY Marc, *Droit des mesures policières: principes généraux, cadre juridique et coopération policière*, Zurich 2008.

RHINOW René, SCHEFER Markus, *Schweizerisches Verfassungsrecht*, 2ème éd., Bâle 2009.

RIBAUX Olivier, Les outils informatisés du renseignement criminel, in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 135-156.

RIEDO Christof, FIOLKA Gerhard, NIGGLI Marcel Alexander, *Strafprozessrecht – sowie Rechtshilfe in Strafsachen*, Bâle 2011.

RIKLIN Franz, Recherchen mit versteckter Kamera: strafrechtlich legal?, *Medialex* 2/2007 p. 55-56 (cité: RIKLIN, Medialex 2007).

RIKLIN Franz, *StPO Kommentar Schweizerische Strafprozessordnung (StPO)*, 2ème éd., Zurich 2014 (cité: RIKLIN, Strafprozessordnung).

RISS Ciril, ZANON Nicole Beranek, Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern, *Jusletter* 9 juillet 2012, n° 4.

ROBINSON Nehemiah, *The Universal Declaration of Human Rights: Its origin, significance, application and interpretation*, New York 1958.

RODRIGUEZ Emilie, L'interprétation des preuves scientifiques par les tribunaux, *RSC* 2/2013 p. 21-32.

ROHMER Sandrine, Banque de données ADN et confidentialité: La constitutionnalité de la législation suisse sur les profils ADN à l'égard du droit au respect de la vie

privée, in Zen-Ruffinen Permarco (éd.), *Les secrets et le* droit, Genève – Zurich – Bâle 2004 (cité: ROHMER, Banque de données ADN).

ROHMER Sandrine, Les enquêtes de grande envergure dans le cadre de la nouvelle loi fédérale sur les profils d'ADN: une proportionnalité douteuse, *RPS* 124 (2006) p. 96-103 (cité: ROHMER, RPS).

ROHMER Sandrine, Nr. 56 Tribunal fédéral, I^re^ Cour de droit public, Arrêt du 23 février 2012 dans les causes Ministère public du canton de Genève contre A. et Madame la Cheffe de la police cantonale genevoise contre A. – 1B_685/2011 et 1B_639/2011, *Forumpoenale* 2012/6 p. 345-348 (cité: ROHMER, Forumpoenale).

ROHMER Sandrine, *Spécificité des données génétiques et protection de la sphère privée*, Thèse de doctorat, Genève – Zurich 2006 (cité: ROHMER, Thèse).

ROSENTHAL David, JÖHRI Yvonne, *Handkommentar zum Datenschutzgesetz: sowie weiteren, ausgewählten Bestimmungen*, 2ème éd., Zurich 2014.

ROSSY Quentin, Définition et méthodes de traitement des situations récurrentes en analyse criminelle: développement d'un catalogue de patterns de visualisation, *RICPTS* LXII (2009) p. 73-74.

ROTH Robert, Admission, administration et appréciation de la preuve: questions choisies, in Jeanneret Yvan, Kuhn André (éd.), *Procédure pénale suisse – approche théorique et mise en oeuvre cantonale*, Neuchâtel 2010, p. 53-72.

ROTH Simon, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, *Jusletter* 17 août 2015 (cité: ROTH Simon).

ROUX Anne-Christine, L'utilisation de l'ADN dans le cadre d'une procédure pénale, in Moreillon Laurent, Kuhn André, Bichovysky Aude, Willi-Jayet Aline, Viredaz Baptiste (éd.), *Aspects pénaux du droit du vivant*, série II, vol. 3, Bâle – Genève, 2004, p. 179-195.

RUCKSTUHL Niklaus, Technische Überwachungen aus anwaltlicher Sicht, *AJP/PJA* 2005 p. 150-158.

RUCKSTUHL Niklaus, DITTMANN Volker, ARNOLD Jörg, *Strafprozessrecht – unter Einschluss der forensischen Psychiatrie und Rechtsmedizin sowie des*

kriminaltechnischen und naturwissenschaftlichen Gutachtens, Zurich – Bâle – Genève 2011.

RUDAZ Carole, De l'utilité de l'investigation secrète dans la lutte contre le "grooming", *Jusletter* 2 décembre 2013.

RUEGG Jean, La vidéosurveillance contre la ville, *Colloque "la ville mal-aimée" du 5 au 12 juin 2007*.

RUEGG Jean, FLÜCKIGER Alexandre, NOVEMBER Valérie, KLAUSER Francisco, *Vidéosurveillance et risques dans l'espace à usage public: Représentations des risques, régulation sociale et liberté de mouvement*, n° 55, Genève 2006.

RÜFENACHT Nathalie, Le système d'assistance ISA ouvre de nouvelles perspectives, *BPA – Objectif de sécurité* 2008/1 p. 4-5.

SAFKO Lon, *The Social Media Bible: Tactics, Tools, and Strategies for Business Success*, 3ème éd., New York 2012.

DE SAUSSURE Sophie, L'IMSI-Catcher: fonctions, applications pratiques et légalité, *Jusletter* 30 novembre 2009, n° 2.

SCHMID Niklaus, Der Beweis im schweizerischen Strafprozessrecht, in Frank Richard (éd.), *Der Beweis im Zivil- und Strafprozess der Bundesrepublik Deutschland, Österreichs und der Schweiz: Mittelbarer oder unmittelbarer Beweis im Strafprozess?*, Zurich 1996, p. 75-96 (cité: SCHMID, Der Beweis).

SCHMID Niklaus, *Handbuch des schweizerischen Strafprozessrechts*, 2ème éd., Zurich – Saint-Gall 2013 (cité: SCHMID, Handbuch).

SCHMID Niklaus, *Schweizerische Strafprozessordnung (StPO): Praxiskommentar*, 2ème éd., Zurich – Saint-Gall 2013 (cité: SCHMID, Praxiskommentar).

SCHMID Niklaus, *Strafprozessrecht: eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes*, 4ème éd., Zurich – Bâle – Genève 2004 (cité: SCHMID, Strafprozessrecht).

SCHMID Niklaus, Verwertung von Zufallsfunden sowie Verwertungsverbote nach dem neuen Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), *RPS* 120 (2002) p. 284-320 (cité: SCHMID, RPS).

SCHNEIDER Jürg, Internet Service Provider im Spannungsfeld zwischen Fernmeldegeheimnis und Mitwirkungspflichten bei der Überwachung des E-Mail-Verkehrs über das Internet, *AJP/PJA* 2005 p. 179-191.

SCHOBLICK Robert, SCHOBLICK Gabriele, *RFID-Radio Frequency Identification*, Poing 2005.

SCHUBARTH Martin, Chatroomproblematik und Versagen des Gesetzgebers, *Jusletter* 13 février 2012, n° 9 (cité: SCHUBARTH, Jusletter).

SCHUBARTH Martin, *Kommentar zum schweizerischen Strafrecht – Besonderer Teil, 3. Band – Delikte gegen die Ehre, den Geheim- oder Privatbereich und gegen die Freiheit – Art. 173-186 StGB*, Berne 1984 (cité: SCHUBARTH, Strafrecht).

SCHWEGLER Ivo, *Datenschutz im Polizeiwesen von Bund und Kantonen*, Berne, 2001.

SCHWEIZER Mark Daniel, *Kognitive Täuschungen vor Gericht*, Zurich 2005 (cité: SCHWEIZER M.).

SCHWEIZER Rainer J., Verfassungsrechtlicher Persönlichkeitsschutz, in Thürer Daniel, Aubert Jean-François, Müller Jörg Paul (éd.), *Verfassungsrecht der Schweiz – Droit constitutionnel suisse*, Zurich 2001, p. 691-706 (cité: SCHWEIZER R.).

SÉDALLIAN Valérie, *Preuve et signature électronique*, Paris 2008, disponible sur : http://www.juriscom.net/ [consulté le 08.05.2016].

SEEGER Pascal, Identification des diffuseurs de fichiers illégaux dans les réseaux de partage de fichiers "peer-to-peer", in Cimichella Sandro, Kuhn André, Niggli Marcel Alexander (éd.), *Neue Technologie und Kriminalität: Neue Kriminologie? – Nouvelles technologies et criminalité: nouvelle criminologie?*, Zurich 2006, volume 24, p. 265-289.

SEILER Martin, *La Suisse a aussi chassé un fantôme, Matériel de prélèvement ADN contaminé*, Zurich 2011.

SKARUPINSKI Philipp, GROSSENBACHER Josefina, Zwischen Schutz und Schranken – polizeiliche Chatroom-Ermittlungen zur Bekämpfung von pädophilen Straftaten, *Jusletter* 3 octobre 2011, n° 2.

SOULLIÈRE Nicole, *Police et technologies: un bilan historique, un regard contemporain*, Ottawa 1999.

ST-YVES Michel (éd.), *Les entrevues d'enquête – L'essentiel*, Cowansville 2014 (cité: ST-YVES-NOM).

STALDER Séverine, VERGÈRES Olivier, 17 Bundesgericht, Incidences de la procédure pénale unifiée sur le travail de la police – Résumé du travail de séminaire réalisé lors des Cours de Conduite III organisés par l'Institut suisse de police (ISP-CC III 2007/2008), *RSC* 2/2009 p. 60-63.

STÄMPFLI Sandra, *Das Schengener Informationssystem und das Recht der informationellen Selbstbestimmung*, Berne 2009.

STRATENWERTH Günter, WOHLERS Wolfgang, *Schweizerisches Strafgesetzbuch – Handkommentar*, 3ème éd., Berne 2013.

STRATENWERTH Günter, JENNY Guido, BOMMER Félix, *Schweizerisches Strafrecht – BT 1 – Straftaten fefen Individualinteressen*, 7ème éd., Berne 2010.

STRÄULI Bernhard, La surveillance de la correspondance par poste et télécommunication: aperçu du nouveau droit, in Cassani Ursula, Dittman Volker, Maag Renie, Steiner Silvia (éd.), *Mehr Sicherheit – weniger Freiheit? – Plus de sécurité – moins de liberté?*, Zurich 2003, volume 21, p. 93-194.

STROBEL Daehyun, *IMSI-Catcher*, Seminararbeit Ruhr-Universität Bochum, Ruhr 2007.

STUCKI Daniel, Die Strafbarkeit von «Phishing» nach StGB, *Jusletter* 9 janvier 2012, n° 2.

TANQUEREL Thierry, *Manuel de droit administratif*, Genève 2011.

TARONI Franco, Interprétation de la preuve ADN : le juriste, le scientifique et les probabilités, in Cassani Ursula, Dittman Volker, Maag Renie, Steiner Silvia (éd.), *Mehr Sicherheit – weniger Freiheit ? – Plus de sécurité – moins de liberté ?*, Zurich 2003, volume 21, p. 273-293 (cité: TARONI, preuve ADN).

TARONI Franco, *La recherche et la gestion des liens dans l'investigation des cambriolages: une étape vers l'exploitation systématique des données de police*, Thèse de doctorat, Lausanne 1997 (cité: TARONI, Thèse).

TARONI Franco, AITKEN Colin, Probabilité et preuve par l'ADN dans les affaires civiles et criminelles. Questions de la cour et réponses fallacieuses des experts, *RPS* 116 (1998) p. 291-313.

TARONI Franco, LAMBERT J.A, FEREDAY Lyn, WERRETT David J., Evaluation and presentation of forensic DNA evidence in European laboratories, *Science & Justice* 42(2002) p. 21-28.

TARONI Franco, MANGIN Patrice, BÄR Walter, Die Interpretation des Beweiswertes von DNA-Untersuchungen in sachverständigen Gutachten, *RPS* 117 (1999) p. 439-445.

THEVENAZ Alain (éd.), *Les preuves*, Berne 2014 (Cité: Preuve-NOM).

THOMANN Eugen, Verdeckte Fahndung aus der Sicht der Polizei, *RPS* 1993 p. 285-306.

THOMPSON William C., Evaluating the Admissibility of New Genetic Identification Tests: Lessons from the "DNA War", *The Journal of Criminal Law & Criminology* 84(1993) n°1 p. 22-104.

THORMANN Olivier, BRECHBÜHL Beat, 5. Titel: Zwangsmassnahmen – 4. Kapitel: Durschungen und Untersuchung, in Niggli Marcel Alexander, Heer Marianne, Wiprächtiger Hans (éd), *Schweizerische Strafprozessordnung – Jugendstrafprozessordnung*, 2ème éd., Bâle 2013, p. 1820-1892.

TILSTONE William J., SAVAGE Kathleen A., CLARK Leigh A., *Encyclopedia of Forensic science: An Encyclopedia of History, Methods, and Techniques*, Santa Barbara 2006.

TRECCANI Jean, Interceptions électroniques, in Cassani Ursula, Dittman Volker, Maag Renie, Steiner Silvia (éd.), *Mehr Sicherheit – weniger Freiheit ? – Plus de sécurité – moins de liberté ?*, Zurich 2003, volume 21, p. 217-238.

TRECHSEL Stefan, *Human Rights in Criminal Proceedings*, 2ème éd., Oxford 2005 (cité: TRECHSEL, Human Rights).

TRECHSEL Stefan, *Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 : Kurzkommentar*, 2ème éd., Zürich 1997 (cité: TRECHSEL, Kurzkommentar).

TRECHSEL Stefan, Struktur und Funktion der Vermutung der Schuldlosigkeit – Ein Beitrag zur Auslegung von Art. 6 Ziff. 2 EMRK, *RSJ* 77 (1981) p. 317-324 et 335-340 (cité: TRECHSEL, RSJ).

TRECHSEL Stefan, PIETH Mark (éd.) *Schweizerisches Strafgesetzbuch – Praxiskommentar*, 2ème éd. (cité: TRECHSEL, PIETH-NOM).

TRÜEB Hans Rudolf, Von Metropolis zum Global Village - Das Verhältnis von Datenschutz und Informationstechnologie, *DIGMA* 2003 p. 64-70.

DE VALICOURT DE SÉRANVILLIERS Héliane, *La preuve par l'ADN et l'erreur judiciaire*, Paris 2009.

DE VELTERE Rennaat, La dactyloscopie, in Leriche Anne (éd.), *La criminalistique: du mythe à la réalité quotidienne*, Bruxelles 2002, p. 129-150.

VERNIORY Jean-Marc, *Les droits de la défense dans les phases préliminaires du procès pénal*, Thèse de docotorat, Berne 2005.

VEST Hans, Schweiz, in Gropp Walter (éd.), *Besondere Ermittlungsmassnahmen zur Bekämpfung der Organisierten Kriminalität*, Freiburg im Breisgau 1993, p. 635-693.

VETTERLI Luzia, Nr. 17 Bundesgericht, I. öffentlich-rechtliche Abteilung, Urteil vom 24. September 2007 i.S. X. gegen Staatsanwaltschaft des Kantons Freiburg, Kantonsgericht Freiburg – 1P_51/2007, *forumpoenale* 2008/2 p. 82-86.

VETTERLI Luzia, Verdeckte Ermittlung und Grundrechtsschutz, *forumpoenale* 2008/6 p. 367-372 (cité: VETTERLI, Verdeckte Ermittlung).

VIAU Louise, La preuve pénale, in Tremblay Lise, Tremblay Jocelyne (éd.), *Droit pénal – Procédure pénale*, Volume 11, Cowansville 2007, p. 103-149 (cité: VIAU, Preuve pénale).

VILLIGER Mark E., EMRK und UNO- Menscgenrechtspakte, in Thürer Daniel, Aubert Jean-François, Müller Jörg Paul (éd.), *Verfassungsrecht der Schweiz – Droit constitutionnel suisse*, Zurich 2001, p. 647-656.

VINCENT Frank H. R., *Report – Inquiry into the circumstances that led to the conviction of Mr Farah Abdulkadir Jama*, Melbourne 2010.

VIREDAZ Baptiste, De l'usage de l'ADN par la justice pénale américaine, in Moreillon Laurent, Kuhn André, Bichovysky Aude, Willi-Jayet Aline, Viredaz Baptiste (éd.), *Aspects pénaux du droit du vivant*, série II, vol. 3, Bâle – Genève, 2004, p. 315-333.

VIREDAZ Baptiste, *Le sentiment d'insécurité : Devons-nous avoir peur?*, Grolley 2005 (cité: VIREDAZ, insécurité).

VITALIS André, *Informatique, pouvoir et libertés*, 2ème éd., Paris 1988.

VOGGENAUER-VON BOTHMER Roland, Welche Daten werden wirklich gebraucht? Bekannte und neue Versicherungsmodelle bezüglich einer laufleistungsabhängigen Tarifierung in der Fahrzeug-Versicherung, *DIGMA* 2007 p. 102-104.

VOGT Beatrice, Opferrechtliche Bestimmungen der Schweizerischen Strafprozessordnung – 4. Abschnitt: Zivilklage – Art. 154, in Fullin Nicolai, Gomm Peter, Schaffner-Hess Susanne, Steiger-Sackmann Sabine, Tamm Nikolaus, Vogt Beatrice, Zehntner Dominik (éd.), *Opferhilfgesetz*, Berne 2009, p. 403-413.

VUILLE Joëlle, L'activité menant au (non-) dépôt d'ADN dans une affaire de viol: critique de l'arrêt du Tribunal fédéral du 7 octobre 2011 6B_150/2011, *forumpoenale* 2012/4, p. 247-252 (cité: VUILLE, forumpoenale).

VUILLE Joëlle, "L'ADN, c'est la signature de Dieu": ce que la justice pénale dit de la preuve génétique, *RSC* 1/2012 p. 3-16 (cité: VUILLE, TARONI, RSC 2012).

VUILLE Joëlle, *Ce que la justice fait dire à l'ADN (et que l'ADN ne dit pas vraiment)*, Thèse de docotorat, Lausanne 2011 (cité: VUILLE, Thèse).

VUILLE Joëlle, TARONI Franco, L'article 184 al. 3 CPP, une fausse bonne idée du législateur, *RPS* 129 (2011) p. 164-179 (cité: VUILLE, TARONI, RPS 2011).

VUILLE Joëlle, TARONI Franco, Le juge et les probabilités – Commentaire du jugement de l'Obergericht du canton de Zurich du 19 août 2008 dans la cause L. contre Stradtrichteramt Zürich, *forumpoenale* 2009/6 p. 365-368 (VUILLE, TARONI, forumpoenale).

WAGNER Klaus, HÜTTL Thomas, BACKIN Dieter, *Einführung Wirtschaftsinformatik: IT-Grundwissen für Studium und Praxis*, Wiesbaden 2012.

WALDER Hans, *Die Beweisfuehrung in Strafsachen, inbesondere der Indizienbeweis*, Zurich 1974.

WALTER Jean-Philippe, Communication de données personnelles à l'étranger, in Epiney Astrid, Hobi Patrick (éd.), *Die Revision des Datenschutzgesetzes - La révision de la Loi sur la protection des données*, Zurich 2009, p. 99-137 (cité: WALTER, Données personnelles).

WALTER Jean-Philippe, Le droit de l'individu à l'autoprotection lors du traitement de données personnelles dans le domaine des télécommunications, in Cottier Bertil (éd.), *Le droit des télécommunications en mutation*, Fribourg 2001, p. 459-482 (cité: WALTER).

WATSON Ian, *The Universal Machine: From the Dawn of Computing to Digital Consciousness*, Berlin 2012.

WEBER Rolf H., FERCSIK SCHNYDER Orsolya, "Was für 'ne Sorte von Geschöpf ist euer Krokodil?" : zur datenschutzrechtlichen Qualifikation von IP-Adressen, *Sic!* 9/2009, p. 577-589.

WELSH Brandon C., FARRINGTON David P., *Home Office Research Study 252 – Crime prevention effects of closed circuit television: a systematic review*, Londres 2002.

WERLEN Bruno, 5. Titel: Zwangsmassnahmen – 6. Kapitel: Erkennungsdienstliche Erfassung, Schrift- und Sprachproben, in Niggli Marcel Alexander, Heer Marianne, Wiprächtiger Hans (éd), *Schweizerische Strafprozessordnung – Jugendstrafprozessordnung*, 2ème éd., Bâle 2013, p. 1999-2007.

WERRETT D.J., L'identification par l'"empreinte génétique", *Revue internationale de police criminelle* 408(1987) p. 21-25.

WERTHEIM Pat A, Scientific Comparaison and Identification of Fingerprint Evidence, *Fingerprint Whorld* 26(2000) p. 95-106.

WIEDERKEHR René, RICHLI Paul, *Praxis des allgemeinen Verwaltungsrechts – Eine systematische Analyse der Rechtsprechung*, Berne 2012.

WIPRÄCHTIGER Hans, Psychatrie und Strafrecht – Was erwartet der Jurist, in Ebner Gerhard, Dittmann Volker, Gravier Bruno, Hoffmann Klaus, Raggenbass René (éd.), *Psychatrie und Recht – Forum gesundheitsrecht*, Zurich 2005, p. 199-226.

XU Guochang, *GPS: Theroy, Algorithms and Applications*, 2ème éd., Berlin – Heindelberg 2007.

ZALUNARDO-WALSER Roberto, *Verdeckte kriminalpolizeiliche Ermittlungsmassnahmen unter besonderer Berücksichtigung der Observation*, Thèse de doctorat, Zürich 1998.

ZOLLINGER Kurt, Augenschein und Gutachten Sachverständiger nach der StPO, *Kriminalistik* 61 (2007) p. 569-571.

ZWIEHOFF Gabriele, *Das Recht auf den Sachverständigen: Beiträge zum strafprozessualen Beweisrecht*, Baden-Baden 2000.

Messages

Message du Conseil fédéral concernant l'adhésion de la Suisse à l'Organisation des Nations Unies (ONU), Berne 21 décembre 1981, FF 1982 I 505, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, ONU).

Message du Conseil fédéral concernant la loi fédérale sur la protection des données (LPD), Berne 23 mars 1988, FF 1988 II 421, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, LPD).

Message du Conseil fédéral concernant le traitement des données en matière de poursuite pénale, Berne 16 octobre 1990, FF 1990 III 1161, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, complémentaire LPD).

Message du Conseil fédéral concernant l'adhésion à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Berne 13 novembre 1996, FF 1997 I 701, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, Convention à l'égard du traitement automatisé).

Message du Conseil fédéral relatif à une nouvelle constitution fédérale, Berne 20 novembre 1996, FF 1997 I 1, disponible sur: http://www.admin.ch [consulté le 08.05.2016] (cité: Message, Constitution).

Message du Conseil fédéral concernant les lois fédérales sur la surveillance de la correspondance postale et des télécommunications et sur l'investigation secrète, Berne 1er juillet 1998, FF 1998 IV 3689, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, LSCPT).

Message du Conseil fédéral relatif à la loi sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification de personnes inconnues ou disparues, Berne 8 novembre 2000, FF 2001 19, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, ADN).

Message du Conseil fédéral relatif à la loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSél), Berne 3 juillet 2001, FF 2001 5423, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, SCSél).

Message du Conseil fédéral relatif à l'unification du droit de la procédure pénale, Berne 21 décembre 2005, FF 2006 1057, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, CPP).

Message du Conseil fédéral concernant la loi sur les systèmes d'information de police de la Confédération, Berne 24 mai 2006, FF 2006 4819, disponible sur: http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, LSIP).

Message du Conseil fédéral relatif la modification de la loi fédérale instituant des mesures visant au maintien de la sureté intérieureinte (LMSI), Berne 15 juin 2007, FF 2007 4773, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, LMSI II).

Message du Conseil fédéral concernant Via sicura, le programme d'action de la Confédération visant à renforcer la sécurité routière, Berne 20 octobre 2010, FF 2010 7703, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, Via sicura).

Message du Conseil fédéral concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), Berne 27 février

2013, FF 2013 2379, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, P-LSCPT).

Message du Conseil fédéral concernant la loi fédérale sur le renseignement (LRens), Berne 19 février 2014, FF 2013 2794, disponible sur : http://www.admin.ch/ [consulté le 08.05.2016] (cité: Message, LRens).

Rapports, Avis, Directives, Aide-mémoire

CENTRE DE SERVICE INFORMATIQUES DU DFJP (CSI-DFJP) – SERVICE DE LA SURVEILLANCE DE LA CORRESPONDANCE PAR POSTE ET TÉLÉCOMMUNICATION (SSCPT), *Rapport explicatif concernant la modification de l'ordonnance sur la surveillance par poste et télécommunication (OSCPT; RS 780.11) ainsi que la modification de l'ordonnance sur les émoluments et indemnités en matière de surveillance de la correspondance par poste et télécommunication (RS 780.115.1)*, Berne 26 octobre 2011, disponible sur: http://www.ejpd.admin.ch [consulté le 08.05.2016] (cité: CSI-DFJP SSCPT).

COMMISSION D'ACCÈS À L'INFORMATION, *La biométrique au Québec: Les enjeux*, Québec juillet 2002, disponible sur: http://www.cai.gouv.qc.ca [consulté 08.05.2016] (cité: CAI, biométrie).

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La technologie d'identification par radiofréquence, doit-on s'en méfier?*, Québec 2006.

COMMISSION D'ENQUÊTE PARLEMENTAIRE (CEP), *Evénement survenus au DFJP : Rapport de la Commission d'enquête parlementaire (CEP)*, Berne 22 décembre 1989, FF 1990 I 593 (cité : CEP, 1989).

COMMISSION D'EXPERTS, *Création d'une banque nationale de données de profils ADN: Rapport final de la Commission d'experts*, Berne 18 décembre 1998, disponible sur : http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité: COMMISSION D'EXPERTS, ADN).

COMMISSION DE RÉFORME DU DROIT DU CANADA, *La surveillance électronique*, Montréal 1986.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Conclusions du contrôle du système de traitement des infractions constatées (STIC) – Rapport remis au*

Premier ministre le 20 janvier 2009, Paris 2009, disponible sur: http://www.cnil.fr [consulté le: 08.05.2016] (cité: CNIL, Conclusion du contrôle du STIC).

COMMITTE ON IDENTIFYING THE NEEDS OF THE FORENSIC SCIENCES COMMUNITY, *Strengthenin Forensic Science in the United States: A Path Forward,* Washington 2009 (Cité: NATIONAL RESEARCH COUNCIL).

CONSEIL DE L'EUROPE, *Dossier législatif n°2: La surveillance des communications téléphoniques et l'enregistrement des télécommunications dans certains Etats membres du Conseil de l'Europe*, Strasbourg mai 1982 (cité : CONSEIL DE L'EUROPE, Surveillance).

CONSEIL DE L'EUROPE – COMITÉ DES MINISTRES, *Document CM (2004) 41 – 924 Réunion – Comité européen pour les problèmes criminels (CDPC)*, Strasbourg 20 avril 2005, disponible sur : http://www.coe.int/ [consulté le 08.05.2016] (cité : CONSEIL DE L'EUROPE, Document CM (2004) 41).

CONSEIL FÉDÉRAL, *Avis du Conseil fédéral sur l'initiative parlementaire: Investigation secrètre. Restreindre le champ d'application des dispositions légale – Rapport de la Commission des affaires juridiques du Conseil national du 3 février 2012*, Berne 23 mai 2012, FF 2012 5183, disponible sur : http://www.admin.ch [consulté le 08.05.2016] (cité: Rapport du Conseil fédéral sur l'initiative n°08.458).

CONSEIL FÉDÉRAL, *Rapport explicatif relatif a la modification de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)*, Berne, disponible sur : http://www.admin.ch [consulté le 08.05.2016] (cité: CONSEIL FÉDÉRAL, Rapport modification LSCPT).

CONSEIL FÉDÉRAL, *Rapport sur l'avant-projet de la loi sur le renseignement (LRens) du 8 mars 2013*, Berne 8 mars 2013, FF 2012 5183, disponible sur : http://www.admin.ch [consulté le 08.05.2016] (cité: Rapport sur l'avant-projet LRens).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), *Rapport de la Commission d'experts "Unification de la procédure pénale" – De 29 à l'unité : Concept d'un code de procédure pénale fédéral*, Berne décembre 1997, disponible sur : http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité : De 29 à l'unité).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), *Rapport explicatif relatif à l'avant-projet d'un code de procédure pénale suisse*, Berne juin 2001, disponible sur : http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité : Rapport explicatif relatif à l'avant-projet).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), *Rapport explicatif relatif à l'avant-projet de modification de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sureté intérieure (LMSI)*, Berne février 2006, disponible sur : http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité : Rapport explicatif LMSI II).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), *Synthèse des résultats de la procédure de consultation sur le rapport et l'avant-projet de modification du code de procédure pénale faisant suite à l'initiative parlementaire (08.458) Investigation secrète. Restreindre le champ d'application des dispositions légales*, Berne décembre 2011, disponible sur : http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité : Initiative parlementaire 08.458 – Synthèse des résultats).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), *Vidéosurveillance exercée en vue d'assurer la sécurité dans les gares, les aéroports et les autres espaces publics*, Berne septembre 2007, disponible sur : http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité : DFJP, Rapport vidéosurveillance).

DÉPARTEMENT FÉDÉRAL DE L'ENVIRONNEMENT, DES TRANSPORTS, DE L'ÉNERGIE ET DE LA COMMUNICATION (DETEC), *Rapport explicatif concernant le projet mis en consultation – Mise en œuvre du programme d'action de la Confédération visant à renforcer la sécurité routière (Via sicura)*, Berne 5 novembre 2008, disponible sur : http://www.bakom.admin.ch/ [consulté le 08.05.2016] (cité : DETEC).

DIRECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION DE LA VILLE DE GENÈVE, *Rapport à l'attention du Conseil administratif – Quid de la vidéosurveillance en Ville de Genève – Constats et perspectives*, Genève février 2008, disponible sur : http://www.ville-geneve.ch/ [consulté le 08.05.2016] (cité : VILLE DE GENÈVE, vidéosurveillance).

GROUPE DE TRAVAIL INTERCANTONAL CHARGÉ DE LA LUTTE CONTRE LES ABUS RELATIFS AUX TECHNIQUES D'INFORMATION ET DE COMMUNICATION, *Modèle de poursuite pénale pour les affaires intercantonales et internationales de cyber-criminalité: Proposition du groupe de travail mis sur pied par la Confédération et les cantons afin d'analyser l'opération "Genesis"*, Berne 2003, disponible sur :

http://www.ejpd.admin.ch/ [consulté le 08.05.2016] (cité: Proposition du groupe de travail).

INSTITUT NATIONAL DES HAUTES ETUDES DE SÉCURITÉ (INHES), *Rapport – La vidéo protection – Conditions d'efficacité et critère d'évaluation*, Paris 2008, disponible sur : http://www.lefigaro.fr/ [consulté le 08.05.2016] (cité: INHES).

OFFICE FÉDÉRAL DE L'ENVIRONNEMENT, DES FORÊTS ET DU PAYSAGE (OFEFP), *Rayonnement non ionisant – Stations de base pour téléphonie mobile (GSM) – Recommandation sur les mesures*, Berne 2002, disponible sur: http://www.bafu.admin.ch [consulté le 08.05.2016] (cité: OFEFP).

OFFICE FÉDÉRAL DE LA COMMUNICATION (OFCOM), Localisation des appels d'urgence dans les réseaux suisses de téléphonie mobile, in *Infomailing* 2005 n° 35, Berne 2005, p. 13 (cité: OFCOM, infomailing 2005).

OFFICE FÉDÉRAL DE LA COMMUNICATION (OFCOM), Localisation des appels d'urgence sur les réseaux suisses de téléphonie mobile, in *Infomailing* 2008 n° 10, Berne 2005, p. 8 (cité: OFCOM, infomailing 2008).

OFFICE FÉDÉRAL DE LA COMMUNICATION (OFCOM), *Prescription techniques et administratives concernant l'acheminement et la localisation des appels d'urgence*, Berne 2009, disponible sur: http://www.bakom.admin.ch [consulté le 08.05.2016] (cité: OFCOM, Localisation).

OFFICE FÉDÉRAL DE LA JUSTICE, avis du 25 juin 1991 – mis à jour le 29 juillet 1992, in *JAAC* 56 (1992) n° 20, p. 164- 170 (cité: OFJ, avis du 25 juin 1991).

OFFICE PARLEMENTAIRE FRANÇAIS D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES (OPECST), *Rapport sur la valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire, Paris 7 juin 2001,* disponible sur : http://www.assemblee-nationale.org/ [consulté le 08.05.2016] *(cité: OPECST, ADN).*

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), Les système de mondiaux de navigation par satellite et l'infrastructure des technologies de l'information, in *Perspective des technologies de l'infromation de l'OCDE – TIC, commerce électronique et économie de l'information*, Paris 2000, p. 183-212 (cité: OCDE).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Aide-mémoire pour la vidéosurveillance effectuée par des particuliers*, disponible sur: http://www.edoeb.admin.ch/ [consulté le 08.05.2016] (cité: PFPDT, Vidéosurveillance).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), "Big Brother" se fait discret, in *Newsletter* 01/2006, disponible sur: http://www.edoeb.admin.ch/ [consulté le 08.05.2016] (cité: PFPDT, Big Brother).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Guide relatif aux systèmes de reconnaissance biométrique*, Berne septembre 2009, disponible sur: http://www.edoeb.admin.ch/ [consulté le 08.05.2016] (cité: PFPDT, Biométrie).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Rapport d'activité 2003/2004* , Berne 2004 (cité: PFPDT, Rapport 2003/2004).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Rapport d'activité 2004/2005* , Berne 2005 (cité: PFPDT, Rapport 2004/2005).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Rapport d'activité 2007/2008*, Berne 2009 (cité: PFPDT, Rapport 2007/2008).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Rapport d'activité 2008/2009*, Berne 2009 (cité: PFPDT, Rapport 2008/2009).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Rapport d'activité 2009/2010* , Berne 2010 (cité: PFPDT, Rapport 2009/2010).

ABREVIATIONS

I. Législation

aCPP/FR	Ancien Code de procédure pénale fribourgeois du 14 novembre 1996
aCPP/GE	Ancien Code de procédure pénale genevois du 29 septembre 1977
aCPP/JU	Ancien Code de procédure pénale jurassien du 13 décembre 1990
aCPP/NE	Ancien Code de procédure pénale neuchâtelois du 19 avril 1945
aCPP/VS	Ancien Code de procédure pénale valaisan du 22 février 1962
aCst/GE	Ancienne Constitution de la République et Canton de Genève du 24 mai 1847
aAFIS-O	Ordonnance fédérale du 21 novembre 2001 sur le traitement des données signalétiques biométriques, RS 361.3
AFIS-O	Ordonnance fédérale du 6 décembre 2013 sur le traitement des données signalétiques biométriques, RS 361.3
aStrv/BE	Ancien Gesetz über das Strafverfahren des Kantons Bern vom 15. März 1995
BÜFP	Voir *LSCPT*
CC	Code civil suisse du 10 décembre 1907, RS 210
CEDH	Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales, RS 0.101
CO	Loi fédérale du 30 mars 1911 complétant le code civil suisse (Livre cinquième: Droit des obligations), RS 220
Convention STE n° 108	Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, RS 0.235.1
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
CPP	Code de procédure pénale suisse du 5 octobre 2007, RS 312.0

Cst	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
Cst/AG	Constitution du Canton d'Argovie du 25 juin 1980, RS 131.227
Cst/AI	Constitution du Canton d'Appenzell Rhodes-Intérieures du 24 novembre 1872, RS 131.224.2
Cst/AR	Constitution du Canton d'Appenzell Rhodes-Extérieures du 30 avril 1995, RS 131.224.1
Cst/BE	Constitution du Canton de Berne du 6 juin 1993, RS 131.212
Cst/BL	Constitution du Canton de Bâle-Campagne du 17 mai 1984, RS 131.222.2
Cst/BS	Constitution du Canton de Bâle-Ville du 23 mars 2005, RS 131.222.1
Cst/FR	Constitution du Canton de Fribourg du 16 mai 2004, RS 131.219
Cst/GE	Constitution de la République et Canton de Genève du 14 octobre 2012, RS 131.234
Cst/GL	Constitution du Canton de Glaris du 1er mai 1988, RS 131.217
Cst/GR	Constitution du Canton des Grisons du 14 septembre 2003, RS 131.226
Cst/JU	Constitution de la République et Canton du Jura du 20 mars 1977, RS 131.235
Cst/LU	Constitution du Canton de Lucerne du 17 juin 2007, RS 131.213
Cst/NE	Constitution de la République et Canton de Neuchâtel du 24 septembre 2000, RS 131.233
Cst/NW	Constitution du Canton de Nidwald du 10 octobre 1965, RS 131.216.2
Cst/OW	Constitution du Canton d'Obwald du 19 mai 1968, RS 131.216.1
Cst/SG	Constitution du Canton de Saint-Gall du 10 juin 2001, RS 131.225
Cst/SH	Constitution du canton de Schaffhouse du 17 juin 2002, RS 131.223
Cst/SO	Constitution du Canton de Soleure du 8 juin 1986, RS 131.221

Cst/SZ	Constitution du Canton de Schwytz du 24 novembre 2010, RS 131.215
Cst/TG	Constitution du Canton de Thurgovie du 16 mars 1987, RS 131.228
Cst/TI	Constitution de la République et Canton du Tessin du 14 décembre 1997, RS 131.229
Cst/UR	Constitution du Canton d'Uri du 28 octobre 1984, RS 131.214
Cst/VD	Constitution du Canton de Vaud du 14 avril 2003, RS 131.231
Cst/VS	Constitution du Canton du Valais du 8 mars 1907, RS 131.232
Cst/ZG	Constitution du Canton de Zoug du 31 janvier 1894, RS 131.218
Cst/ZH	Constitution du Canton de Zurich du 27 février 2005, RS 131.211
DUDH	Déclaration universelle des droits de l'homme
EMRK	Voir *CEDH*
LCR	Loi fédérale du 19 décembre 1958 sur la circulation routière, RS 741.01
LFRC	Loi fédérale du 3 octobre 2008 sur le renseignement civil, RS 121
LIPAD/GE	Loi genevoise du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles, RS/GE A 2 08
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure, RS 120
Loi sur les profils d'ADN	Loi fédérale du 20 juin 2003 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues, RS 363
LPD	Loi fédérale du 19 juin 1992 sur la protection des données, RS 235.1
LPol/GE	Loi genevoise du 9 septembre 2014 sur la Police, RS/GE F 1 05
LSCPT	Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication, RS 780.1

LSIP	Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération, RS 361
LTC	Loi du 30 avril 1997 sur les télécommunications, RS 784.10
O-IPAS	Ordonnance du 15 octobre 2008 sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police, RS 361.2
O-JANUS	Ordonnance du 15 octobre 2008 sur le système informatisé de la Police judiciaire fédérale, RS 360.2
O-RIPOL	Ordonnance du 15 octobre 2008 sur le système de recherches informatisées de police, RS 361.0
OAAE	Ordonnance du 23 septembre 2011 sur l'acte authentique électronique, RS 943.033
OIT	Ordonnance du 14 juin 2002 sur les installations de télécommunication, RS 784.101.2
Ordonnance sur les profils d'ADN	Ordonnance du 3 décembre 2004 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues, RS 363.1
OSCPT	Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication, RS 780.11
LRens	Loi du 25 septembre 2015 sur le renseignement, non entrée en vigueur
Pacte II	Pacte international du 16 décembre 1966 relatif aux droits civils et politiques, RS 0.103.2
PPM	Procédure pénale militaire du 23 mars 1979, RS 322.1
StGB	Voir *CP*
StPO	Voir *CPP*

II. Autres abréviations

2D	Deux dimensions
3D	Trois dimensions
ADN/DNA	Acide désoxyribonucléique
ADSL	Asymmetric digital subscriber line
AFIS	Automated fingerprint identification system
AJP/PJA	Aktuelle juristische Praxis - Pratique juridique Actuelle

al.	Alinéa(s)
AP-	Avant-projet
ARPANET	Advanced research projects agency network
art.	Article
ASA	Archives de droit fiscal suisse
ATF	Arrêt du Tribunal fédéral
AUTONAV	Auto navigation
BGH	Arrêt du Bundesgerichtshof
BJM	Basler juristische Mitteilungen
BTS	Base Transceiver Station
BVerfG	Arrêt du Bundesverfassungsgericht
CEP	Commission d'enquête parlementaire
CNIL	Commission nationale de l'informatique et des libertés
CODIS	Combined DNA index system
ComEDH	Commission européenne des droits de l'homme
CourEDH	Cour européenne des droits de l'homme
CSI	Centre des services informatiques
DEP	Le droit de l'environnement dans la pratique
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFJP	Département fédéral de justice et police
éd.	Edition
ETSI	European Telecommunications Standards Institute
fasc.	Fascicule
FBI	Federal bureau of investigation
Fedpol	Office fédéral de la police
FF	Feuille fédérale
FNAEG	Fichier national automatisé des empreintes génétiques
GPS	Global positioning system
GSM	Global system for mobile
HTML	Hypertext markup language
HTTP	Hypertext transfer protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INHES	Institut national des hautes études de la sécurité
IP	Internet protocol
ISA	Intelligent speed adaptation
ISDN	Integrated services digital network
ISO	International Organization for Standardization

JAAC	Jurisprudence des autorités administratives de la Confédération
JdT	Journal des tribunaux (suisses)
let.	Lettre(s)
LIS	Lawful Interception System
LR	Likelihood ratio
MAC	Media Access Control
MMS	Multimedia messaging service
MSISDN	Mobile Station ISDN
N	Numéro de paragraphe
n.	Note de bas de page
n°	Numéro(s)
NAVSTAR	Navigation satellite timing and ranging
NSFNet	National science foundation network
OCDE	Organisation de coopération et de développement économiques
OFCOM	Office fédéral de la communication
OFEFP	Office fédéral de l'environnement, des forêts et du paysage devenu l'OFEV (Office fédéral de l'environnement)
OFJ	Office fédéral de la justice
OFROU	Office fédéral des routes
OFS	Office fédéral de la statistique
OGer	Arrêt de l'Obergericht
ONU	Organisation des Nations Unies
OPECST	Office parlementaire français d'évaluation des choix scientifiques et technologiques
P-	Projet
p.	Page(s)
PCR	Polymerase chain réaction
PFPDT	Préposé fédéral à la protection des données et à la transparence
PJA	Pratique juridique actuelle
PTT	Postes, téléphones, télégraphes
RAMAC	Random access method of accounting and control
RFID	Radio Frequency Identification
RICPTS	Revue internationale de criminologie et de police technique et scientifique
RIPC	Revue internationale de police criminelle

RIPOL	Système de recherches informatisées de police
RJB	Revue de la société des juristes bernois
RJJ	Revue jurassienne de jurisprudence
RPS	Revue pénale suisse
RS	Recueil systématique du droit fédéral
RS/GE	Recueil systématique du droit genevois
RSC	Revue suisse de criminologie
SCOCI	Service de coordination de la lutte contre la criminalité sur Internet
SCPT	Service de la surveillance de la correspondance par poste et télécommunication
SEC	Swiss Experts Certification
SGBD	Système de gestion de base de données
SGBDR	Système de gestion de base de données relationnel
SIM	Subscriber Identity Module
SJ	Semaine judiciaire
SJZ	Schweizerische Juristen-Zeitung
SMS	Short message system
SNDMSG	Send message
SRC	Service du renseignement de la Confédération
ss	Suivant(s)
STRs	Short Tandem Repeats
T.	Tome
TCP	Transmission control protocol
TCP/IP	Transmission control protocol/Internet protocol
TF	Arrêt du Tribunal fédéral non publié
TPF	Arrêt du Tribunal pénal fédéral
TRANSIT	Time ranging and sequential
UIT	Union internationale des télécommunications
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VIH	Virus de l'immunodéficience humaine
Vol.	Volume
VoIP	Voice over IP
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WPA	Wi-Fi Protected Access
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZR	Blätter für Zürcherische Rechtsprechung